Visual Plus Corporation

http://www.visual-plus.com

PROS CS

Version 1.0.1

User Manual

Copyright © 2014 XPR

Table of Contents

Introduction 6
Installation guide 7
- **Server Setup** 9
- **Client Setup** 12

Getting Started 15
- **Starting** 15
- **Create a Portal** 16
- **Adding a control panel** 17
- **Adding a user** 17
- **Upload users to a controller** 18

Manual 20
- **Program menu** 20
  - Display options 20
  - Wiegand configuration 21
  - System parameters 22
  - Client Parameters 23
  - Web server 23
  - Automatic Evacuation report printing 24
  - Scheduled tasks 25
  - Mail settings 27
  - Export 27
  - Pending Updates 28
  - USB Dongle Registration 29
  - Servers 30
  - Restart Server 32
  - Memory Status of Biometry Readers 32
  - Delete Expired Users from all Biometry Readers 33
  - Find users 33
- **Hardware settings** 34
  - Portals 34
    - What is a portal? 34
    - Hardware 34
    - Add a Serial Portal 35
    - Add a Network portal 36
    - Search network portals 37
    - Configure the portal 38
    - Edit a portal 40
    - Delete a portal 41
    - Firmware update 41
  - Control panels 42
    - Add a controller 42
    - Edit a controller 43
    - Start/stop pooling 47
    - Upload configuration to a controller 47

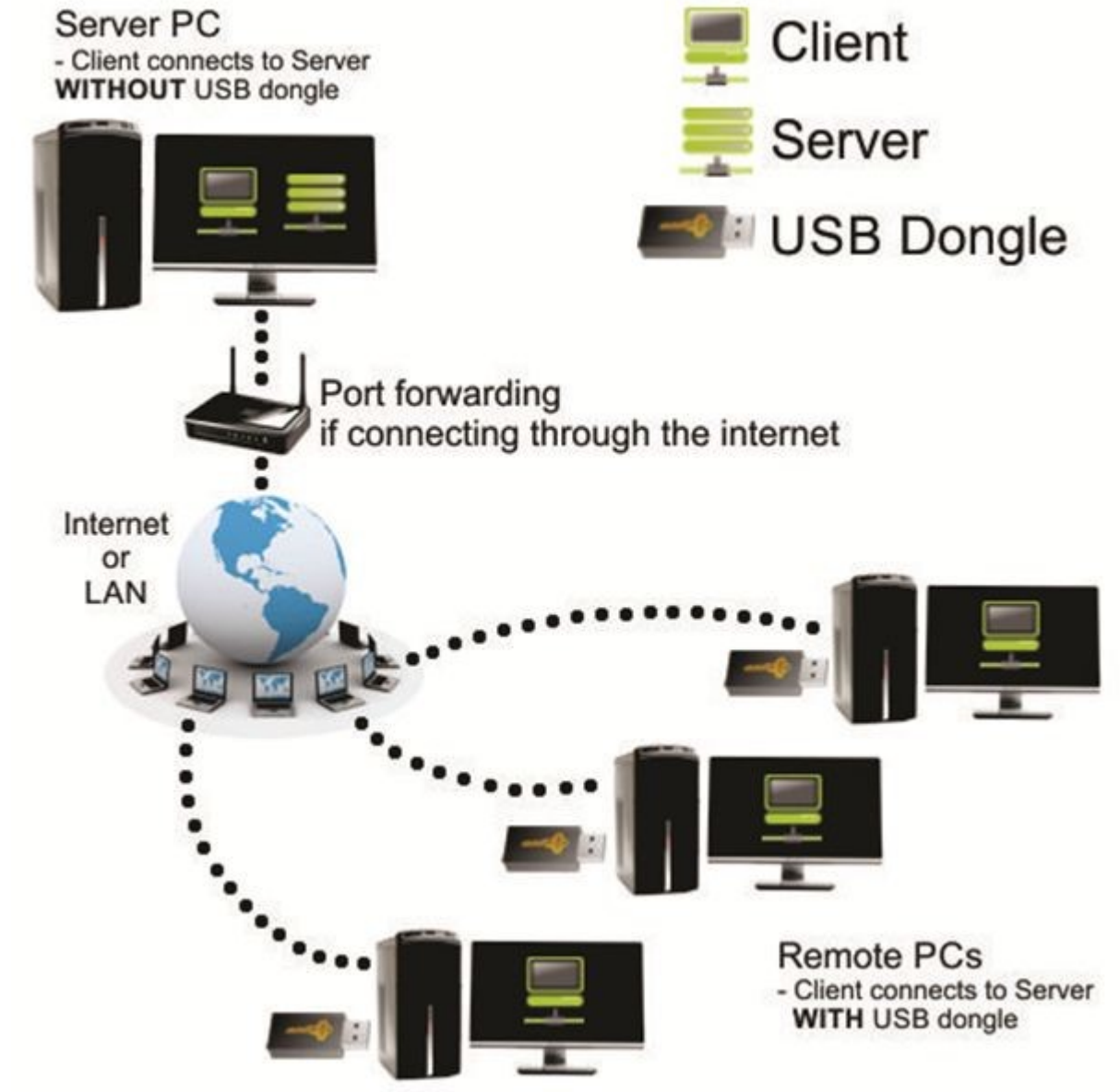
Set controller time 47
Upload users database 47
Firmware update 47
Check firmware version 48
Copy controller settings 48
Doors 49
Door control 52
Readers 52
Fingerprint readers 54
Add or modify a reader 54
Check firmware version 56
Firmware update 56
Read reader settings 57
Upload configuration to a reader 57
Sensor calibration 57
Delete All users from reader 58
Upload all users to reader 58
Delete pending updates 58
Delete Expired users from reader 58
Inputs 58
Outputs 60
Output control 61
Function cards 62
Sites 62
Areas 63
Maps 64
Using the maps 65
Access settings 66
Access levels 66
Adding Access level 66
Edit access level 67
Delete Access Level 67
Departments 67
Add a Department 67
Edit a Department 68
Delete a Department 68
Users 68
Add a user 69
Edit a user 70
Delete a user 70
Fingerprints 71
Read me first 71
Enrolling Fingerprints from a reader 71
Enrollment from a desktop Reader 73
Uploading the fingerprints to the Fingerprint readers 73
Deleting Fingerprints 74
Deleting all users from the fingerprint Reader 74
Deleting user finger templates from the Software 74
Upload all fingerprints to reader 74
Reports 74
User list report 75

Access reports 75
Load report window 75
Set time filters 76
User report 77
Unknown ID report 77
Department report 78
Adding a reader filter to Access report 78
Adding a Doors filter to Access report 79
Adding an Areas filter to Access report 79
Adding a Site filter to Access report 80
Saved report template 80
I/O reports 81
Load report window 81
Set time and controllers filters 81
Inputs report 82
Outputs report 82
Doors report 82
HardwareReport 83
Evacuation report 83
System reports 84
Program operators 85
Add an operator 87
Edit an operator 92
Delete an operator 92
Time and Attendance 92
Workgroups 93
Shifts 93
Public holidays 95
All day absences 97
Reports 98
Edit Reports 99
User report 100
Department report 100
Add a Period filter to reports 101
Add a Day filter to reports 101
Add a Event filter to report 101
Calculation 102
Automatic Calculation 103
Manual Punch 103
Function cards 104
Web report server 105
Access & Attendance report 105
Basic filter 105
Time filter 105
User report 106
Department report 106
Access additional filter 107
T & A filter 108
Reports options 109
Troubleshouting 110

Biometry **110**
Glossary **113**

Introduction

PROS CS is Client-Server based software. The server is installed only in one PC (together with the client) and the client can be installed on more PCs (without installing the server on those PCs). The client running on the same PC as the server does not require USB Dongle to connect to the server. The client running on a remote PC requires USB Dongle to connect to the server.
If you use the client from a remote PC, port forwarding needs to be done so the client can connect to the server. This is done in the router connected to the Internet. The Ports that need to be forwarded can be found in the Server configuration.



.

Installation guide

1. You can install the following products with PROS CS setup:
   - Client only
   - Client + Server
   - Client + Server + Web Server (for generating reports only)

2. UPGRADING from PROS Plus to PROS CS

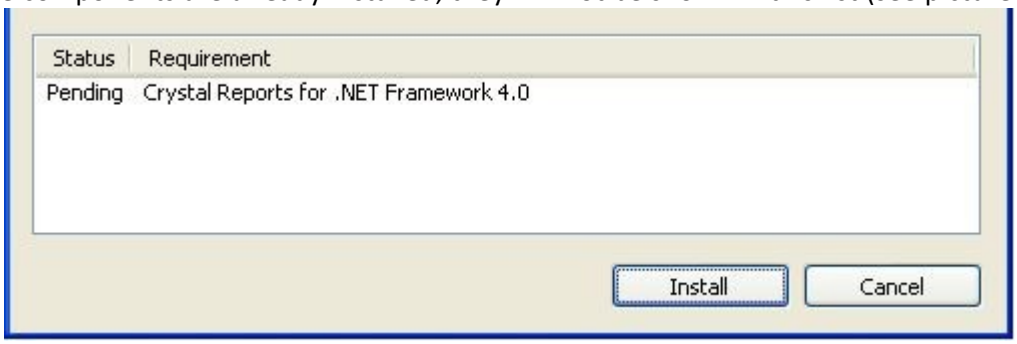
If you are already using PROS Plus and want to upgrade to PROS CS, all you need to do is uninstall PROS Plus and install PROS CS to the same location.

Important note: After uninstalling PROS Plus - do not move/delete the database folder and its contents. PROS CS will continue using the same database as PROS Plus.

3. PROS CS Installation steps

3.1. Installation requirements

PROS CS requires additional components to be installed in order to work properly. If some of the components are already installed, they will not be shown in this list (see picture bellow).



3.2. Installation folder

PROS CS installation folder can be changed during installation

3.3. PROS CS Products

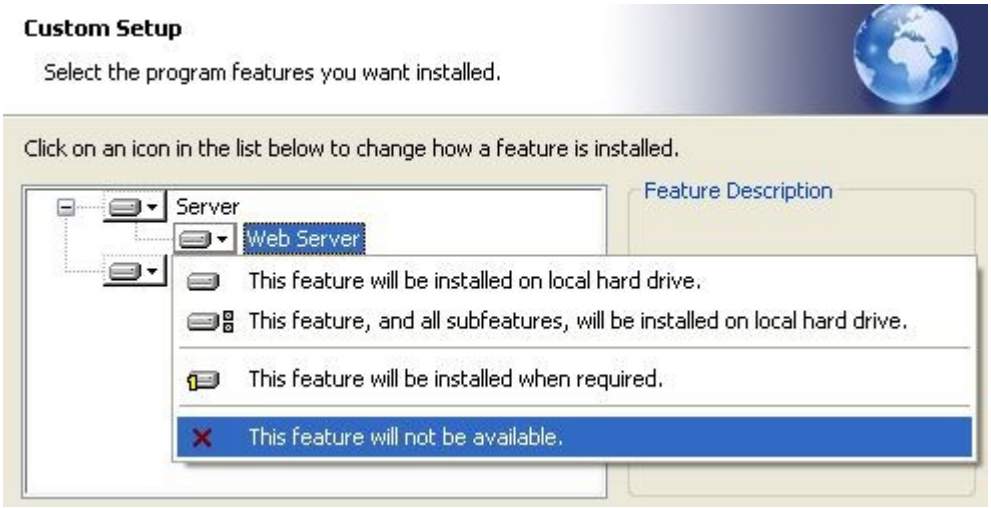
There are three products included in the PROS CS setup: Client, Server and Web Server.

- Client is the software that connects to the Server and it is used for configuring and maintaining hardware, users and other configurations.

- Server is the software that communicates with the hardware and the clients (Client software) and reads/writes data into the database.

- Web Server is the software used for generating reports from an internet browser (Internet Explorer, Google Chrome, Mozilla Firefox….).

The installation of the Server and Web Server is optional and if it is not required you can choose “This feature will not be available” from the setup window.


Custom Setup
Select the program features you want installed.
Click on an icon in the list below to change how a feature is installed.
Feature Description
Server
Web Server
This feature will be installed on local hard drive.
This feature, and all subfeatures, will be installed on local hard drive.
This feature will be installed when required.
This feature will not be available.

3.4. Database requirements

PROS CS can run either with Access 2007 database or with SQL database.

If it runs with Access database NO extra configuration or installation is needed.

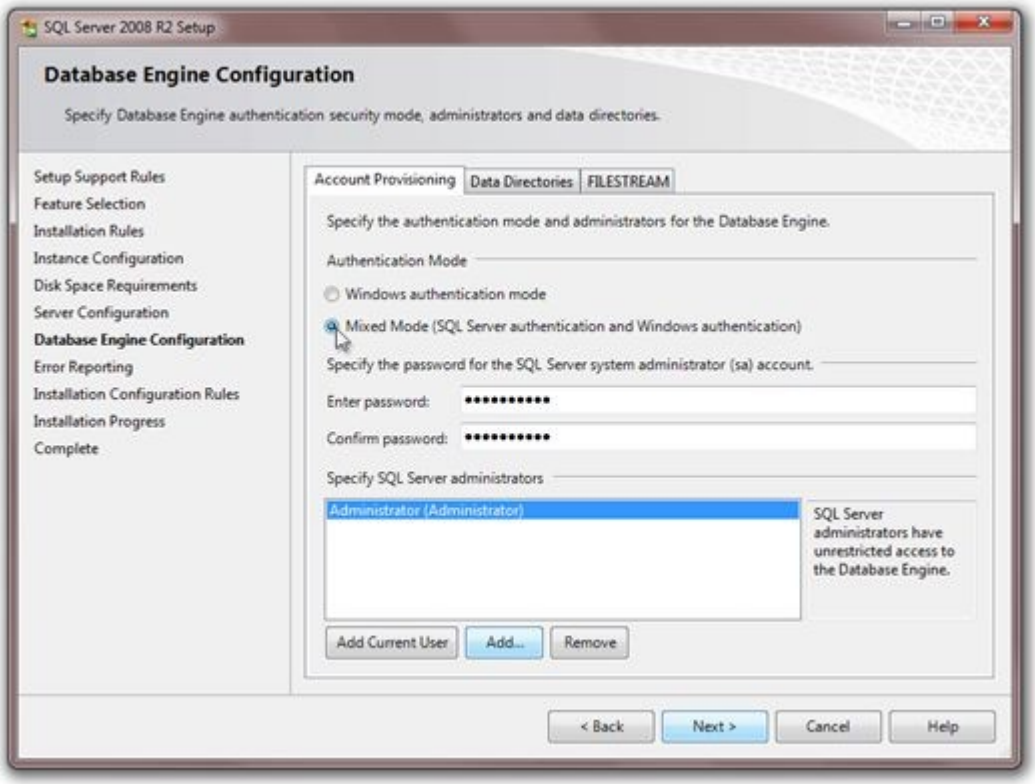
If it runs with SQL database and the database will be placed on the same PC as the Server, then installation of SQL Server Express is required. The setting shown on the picture bellow MUST be set when installing SQL Server. The password entered in the field is required (should write it down for future use of SQL Server). All other settings should be left as their default values.

Minimum SQL requirements are SQL Server 2008 R2 or SQL Express 2008 R2.

SQL Express 2008 R2 can be downloaded from

http://www.microsoft.com/en-us/download/details.aspx?id=30438

(Download the file - SQLEXPRWT_x86_ENU.exe).



Server Setup

Making changes to Server configuration and changing the Database type (SQL or Access) is done with PROS CS **Setup**.
(**Start->All Programs->XPR->**PROS CS->PROS CS **Setup**)
Default values for login are:

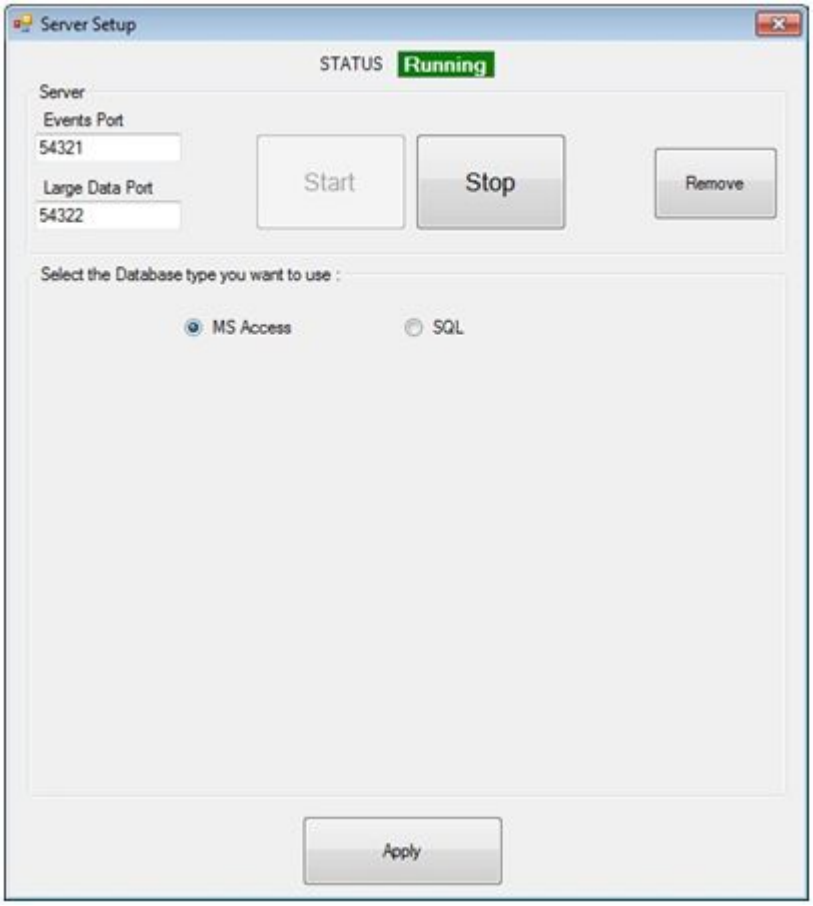
- Operator name: Admin
- Password: admin

and can be changed later in the Client.

1. Server Configuration

In the Server Setup window you can see the Server **status** in the top of the window, the **ports** used for communication between the Client and the Server, and the buttons for starting, stopping and removing the Server **service (The Server is running as a windows service, not as a standard windows application).**

After installing the Server, it is started automatically so you don't need to do extra configuration. But, if you can't connect with the Client to the Server, please first check the server status if it is RUNNING.



- **START** button –**registers** the Server as a windows service and **starts** it immediately
- **STOP** button –**stops** the Server
- **REMOVE** button –**stops** the Server and **removes** it from windows services

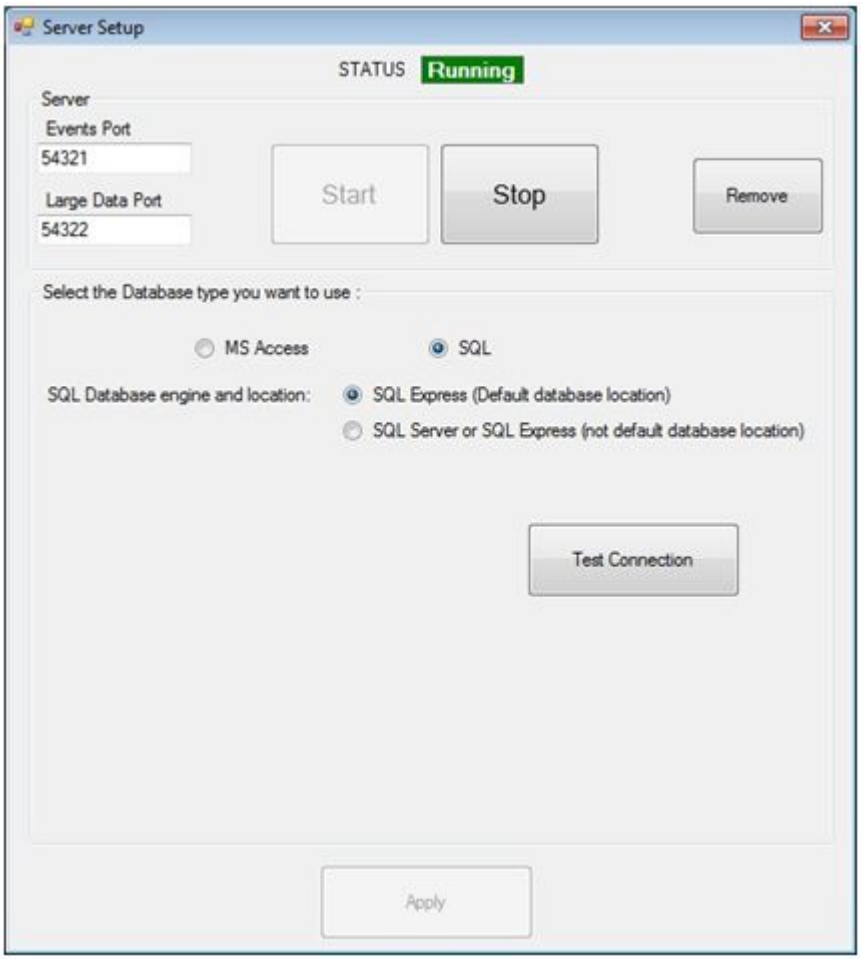
Note: You don't need to press the APPLY button after pressing the START, STOP or REMOVE button.

2. Database configuration

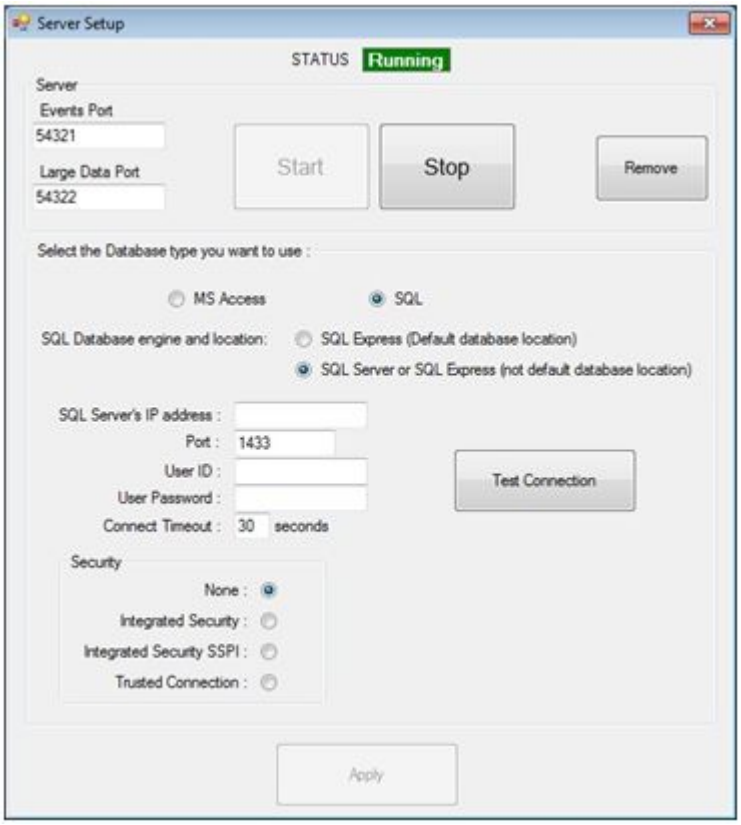
If you want to change the Database type used for storing data in the software you can choose from the options either MS Access or SQL.

WARNING: When switching from Access to SQL or from SQL to Access – data is not transferred. You will have to enter all hardware and user configuration manually.

If SQL is chosen the following screen appear



SQL database can be at its default location (in PROS CS installation folder) and attached to local SQL Server Express or it can be on a remote SQL Server and attached to it (the location of the database that needs to be attached on the remote SQL Server is: "XPR\PROS Plus\Blank Database"). If second option is chosen the following screen appears



Here, SQL Server address and login credentials are entered (these settings are provided by the SQL Server administrator).
After choosing SQL database location, connection with the server must be tested (**Test Connection** button) so that the settings can be applied.

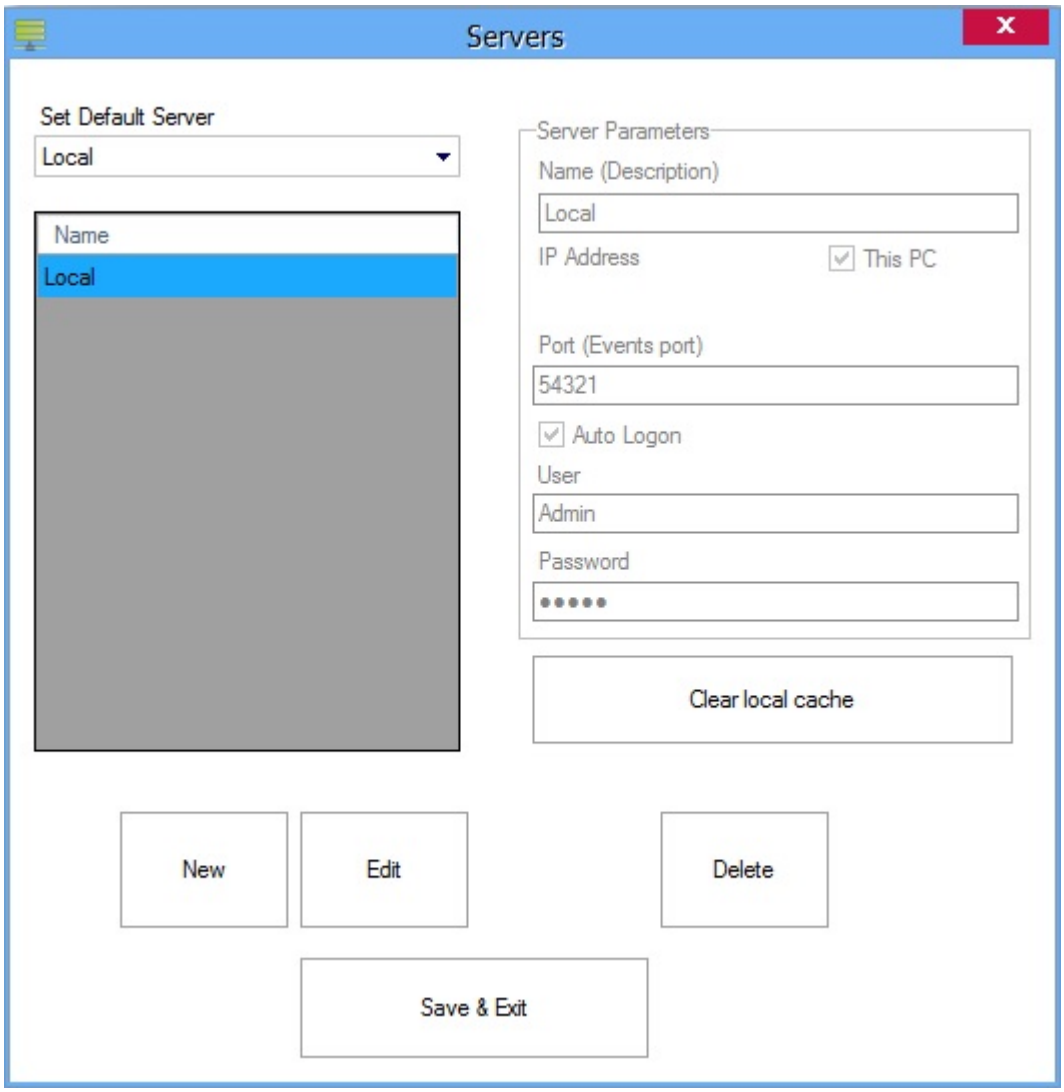
After this dialog appears, **Apply** button is enabled and database setup is finished. If some error dialog box appears instead of the one in the picture, something is not set correctly. Most common issues are:

- SQL Server is not installed on local PC (if **Default database location** chosen)
- SQL Server is installed but authentication mode is **Windows authentication mode**– not **Mixed** mode
- Problem in **local network/internet connection** (if **Not default database location** chosen).
- Not all parameters are correct – IP Address, Port, User, Password, Security… (if **Not default database location** chosen).

Client Setup

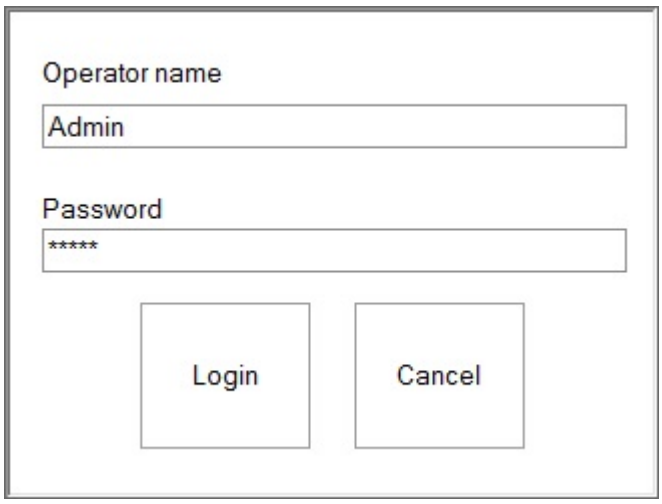
Client setup is made through the menu Settings->Servers. Here you can change or add new Servers. The default server is Local (Local = the Client is on the same PC as the Server). If your Server is on a remote PC (not the same PC as the Client) then you will need to add new Server with the IP address of the remote PC

and the port (Events port) configured in the Server Setup (default is 54321).



Client keeps local cache for each Server in order to speed up the connecting procedure with the server (necessary data for client to run is taken from the Server only once, and each next connection takes only the new changes made)
After configuring the Servers, you can choose a Server from the “Connect To” menu in the top-right corner of the Client. You can connect to other Server without closing the Client by clicking the Disconnect button and then choose a server in the dropdown list. If you want to see info about the current server, just click on the icon next to the “Connect To” menu and an info window will be displayed onscreen.

If "Auto Logon" is not checked for the current server, when connecting a login window appears onscreen asking for credentials. (The default setting is Operator name = "Admin" and Password = "admin")

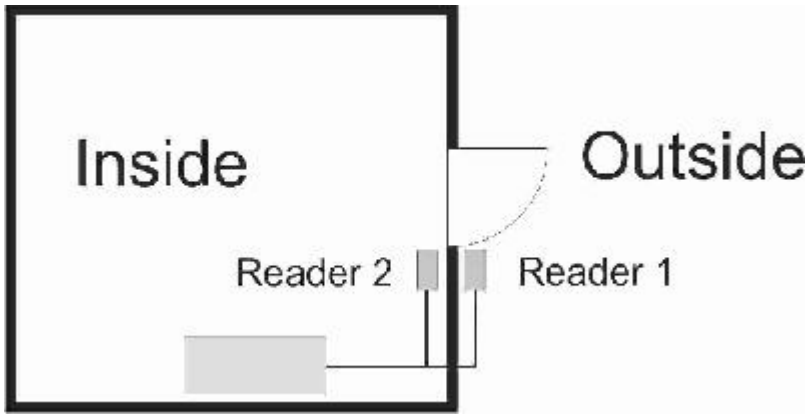

Operator name
Admin
Password
*****
Login
Cancel

Getting Started

This Getting Started Guide will use examples to guide you through the minimum configuration required after installing PROS CS.
This example assumes that the system contains the following elements:

1. Access controller EWSi (2 Reader controller with a built-in CNV1000 TCP/RS485 network converter), controlling main entry to the building with Reader 1 outside and Reader 2 inside.

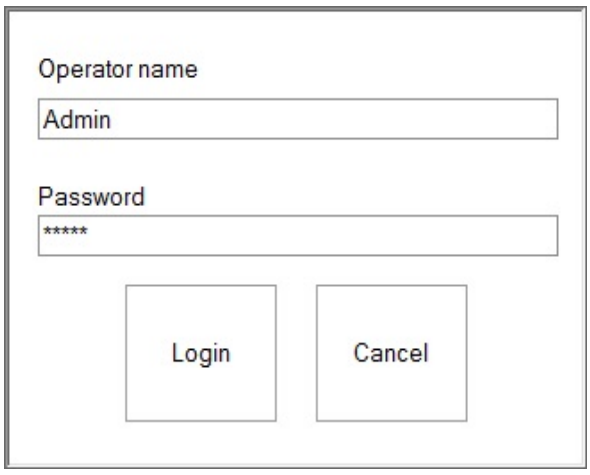
2. Both readers should be standard proximity readers with a Wiegand 26 bit interface.



Starting

- Run the Client
  Select Client from the **Start>All Programs>XPR>PROS CS** menu or double-click on the Client icon on your desktop.

- When connecting to the server, If "Auto Logon" is not checked for the current server a login window will appear asking for credentials. (The default setting is Operator name = "Admin" and Password = "admin")



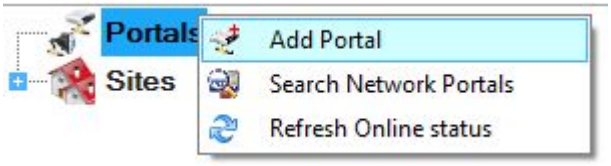
- If you are using the Client to connect to a Server that is on a remote PC then a USB Dongle is required to connect to the Server. If there is none USB Dongle attached to the PC the following message will appear.

-

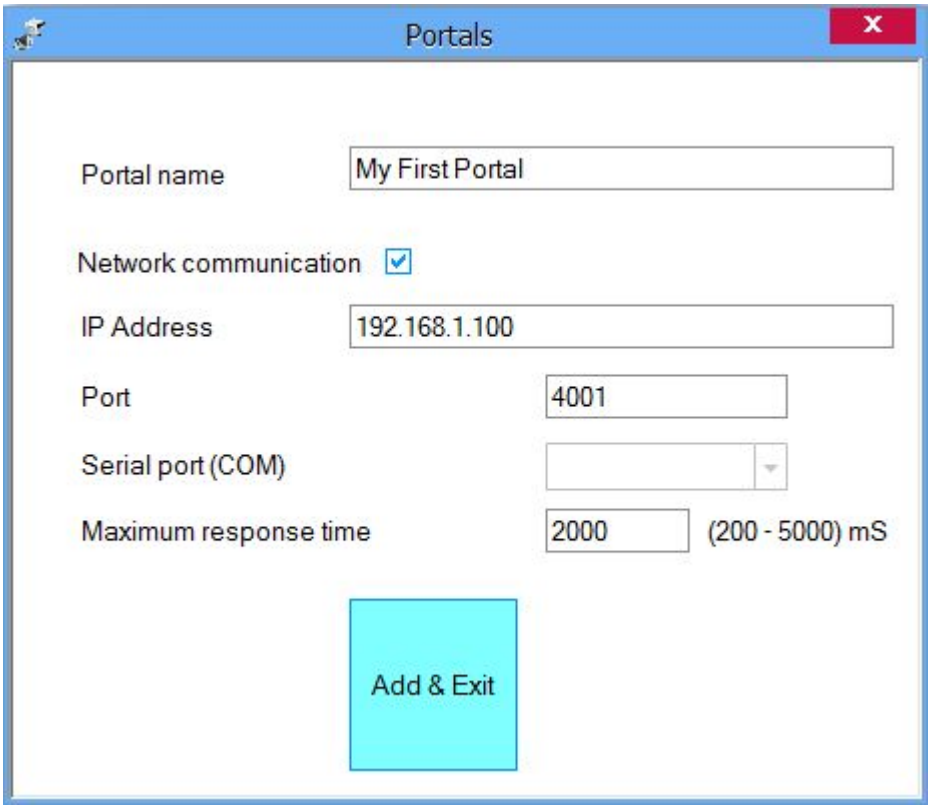
The USB Dongle must be registered at the Server.(**Settings > USB Dongle Registration** from the main menu

Create a Portal

- Right-click on the **Portals** item and select **Add portal**



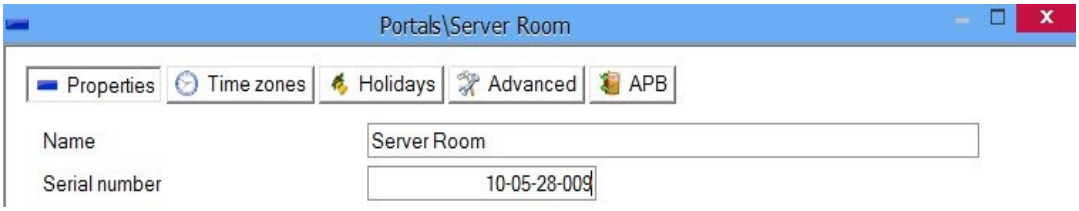
- Consult your installer for the portal IP address and Port, and fill in the Portal properties window with the data.



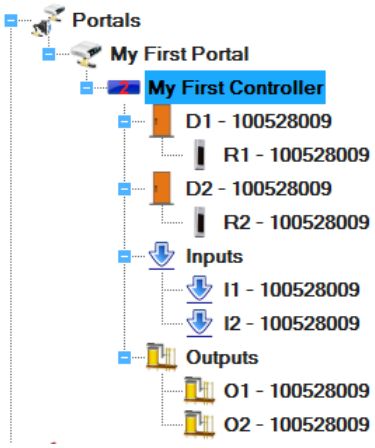
- Click on **Add & Exit**
- The new portal will be shown below the Portals item

Adding a control panel

- Right-click on the new portal item and select **Add controller>EWS**
- Consult your installer for the controller Serial number and fill in the controller properties window with the data.

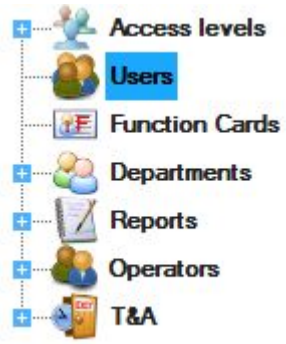


- Click on **Save & Exit** button
- The new controller and controller peripherals are shown under the portal item.

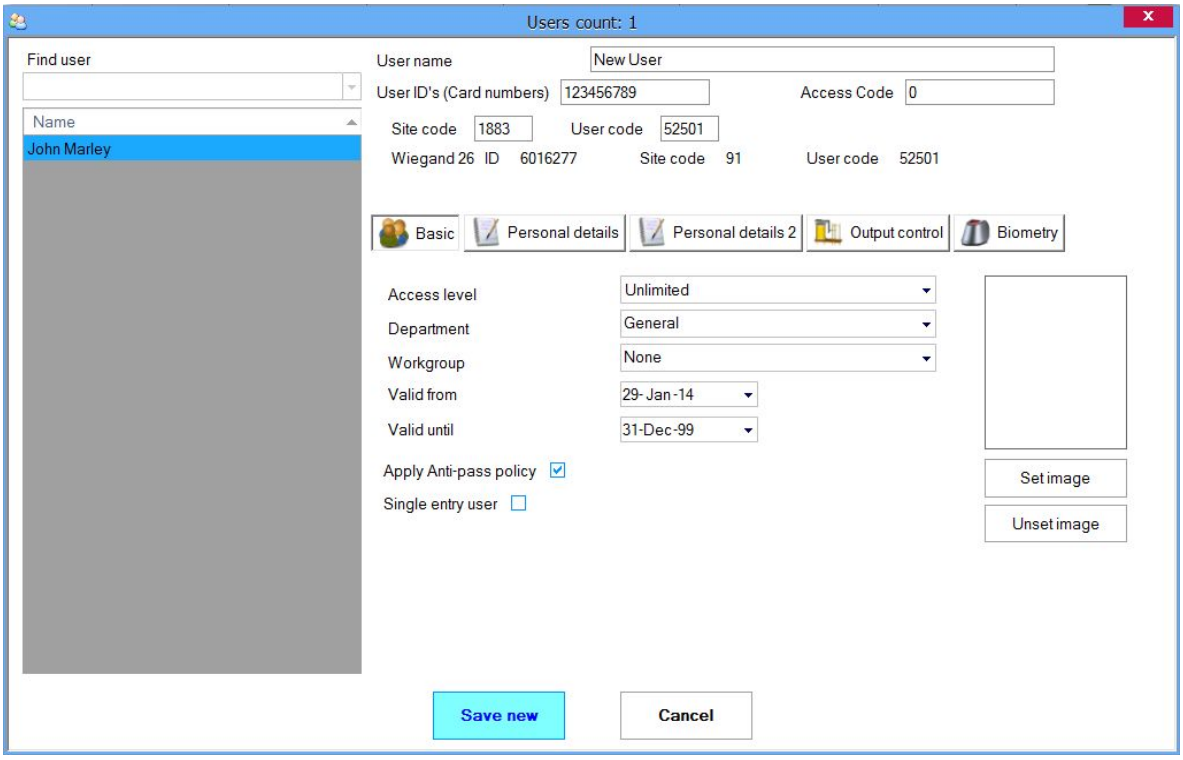


Adding a user

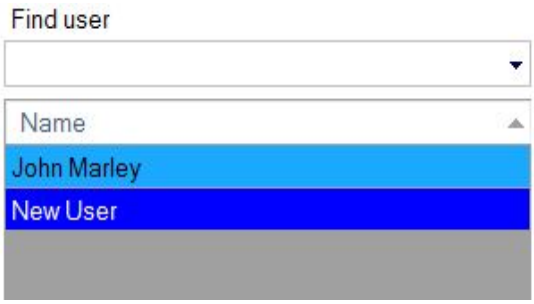
- Double-click on the **Users** item



- On the Users window click on **New user**. The button caption will change to "Save".
- Enter the Name of the user, the user ID (card number), select Unlimited in the Access level drop-down list box, select General in the Department drop-down list box and select the validity period from-until.

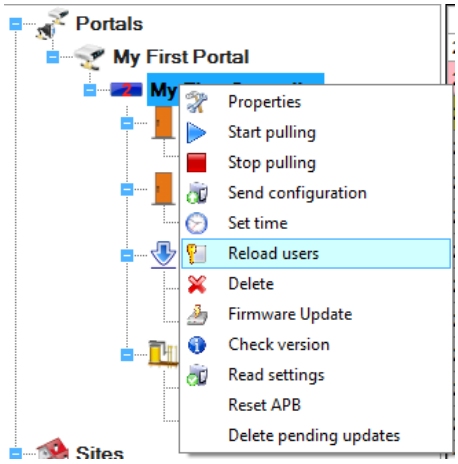


- Click on **Save**
- The entered user will be added to the user table on the left



Upload users to a controller

- Users are automatically added to all controllers according to their Access Level when you add them to the software (or change them). Setting the Access Level of the user to "Unlimited" means that user will be uploaded to all controllers.
- If you want to manually to load the users to one controller - right-click on the controller item and select **Reload users**



- Information about the controller update will be added to the event table

Time	Portal	Controller	Reader	Door	Event	User
29-Jan-14 12:06:41 PM	My First Portal	My First Controller			Load users finished	
29-Jan-14 12:06:41 PM	My First Portal	My First Controller			Loading users	100 %
29-Jan-14 12:06:41 PM	My First Portal	My First Controller			Loading users	
29-Jan-14 12:06:41 PM	My First Portal	My First Controller			Clear keys	OK

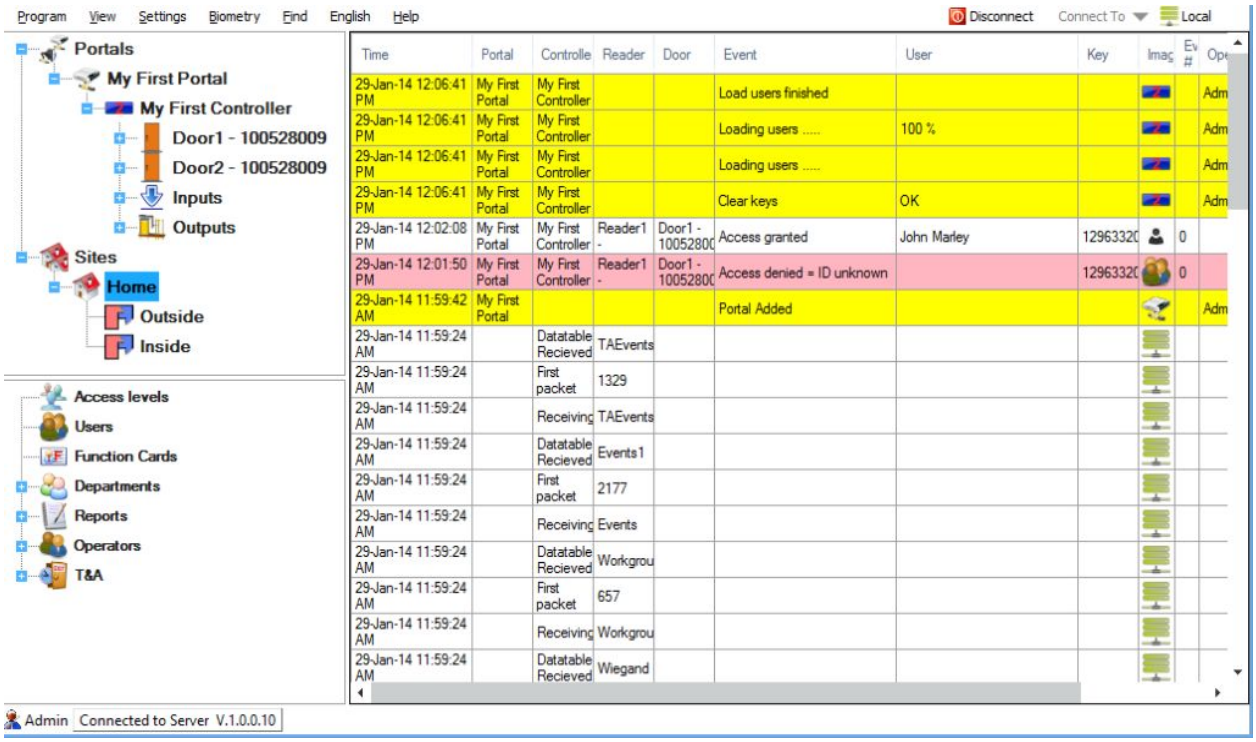
Manual

Program menu

Display options

Display panels

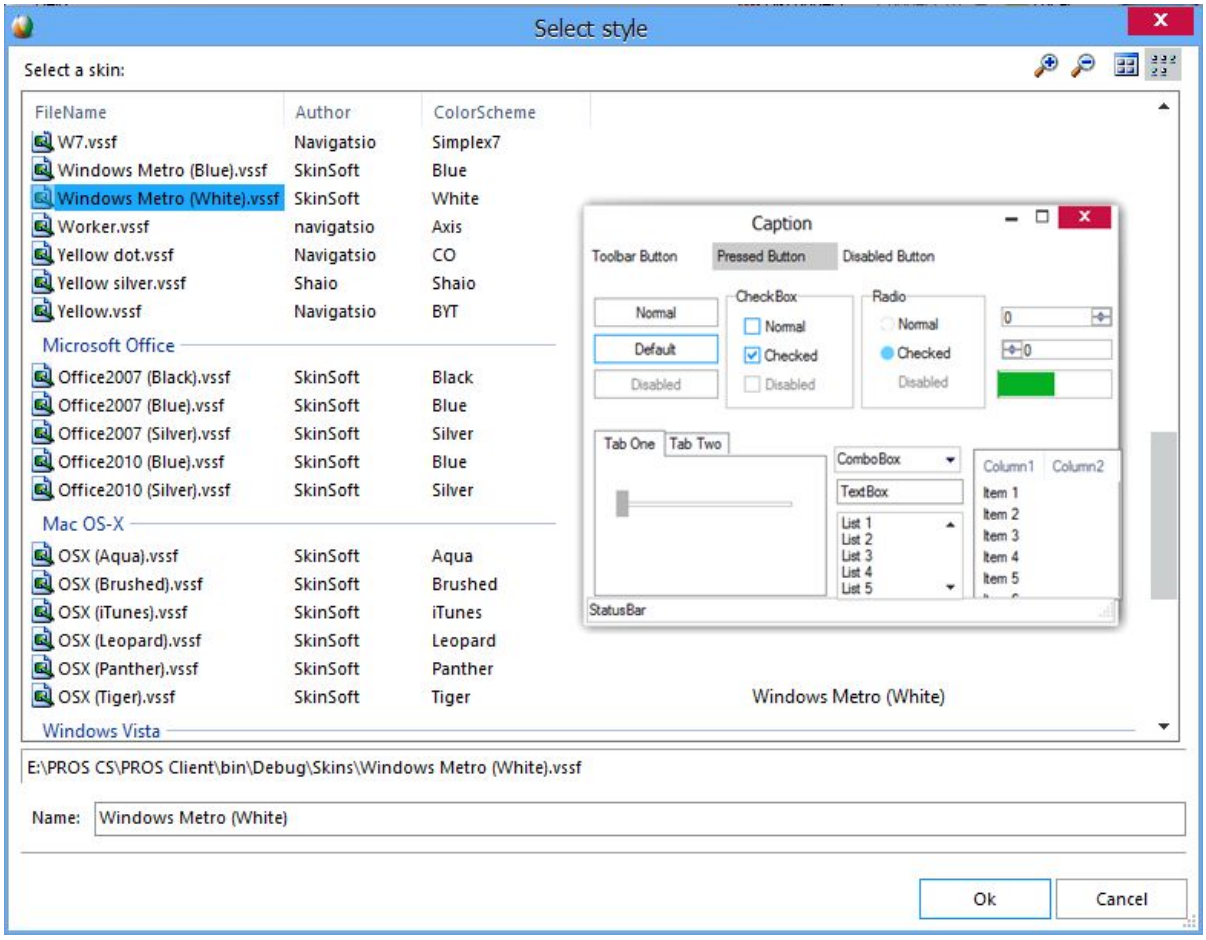
Client's main area is divided into Hardware management, Users management and Events displaying panels.



Each panel can be hidden or made visible by using options in the **View** menu**.**

Display style

Visual appearance can be selected from the menu **View>Appearance>Style**



The Style is stored in the Client and is loaded at client startup.

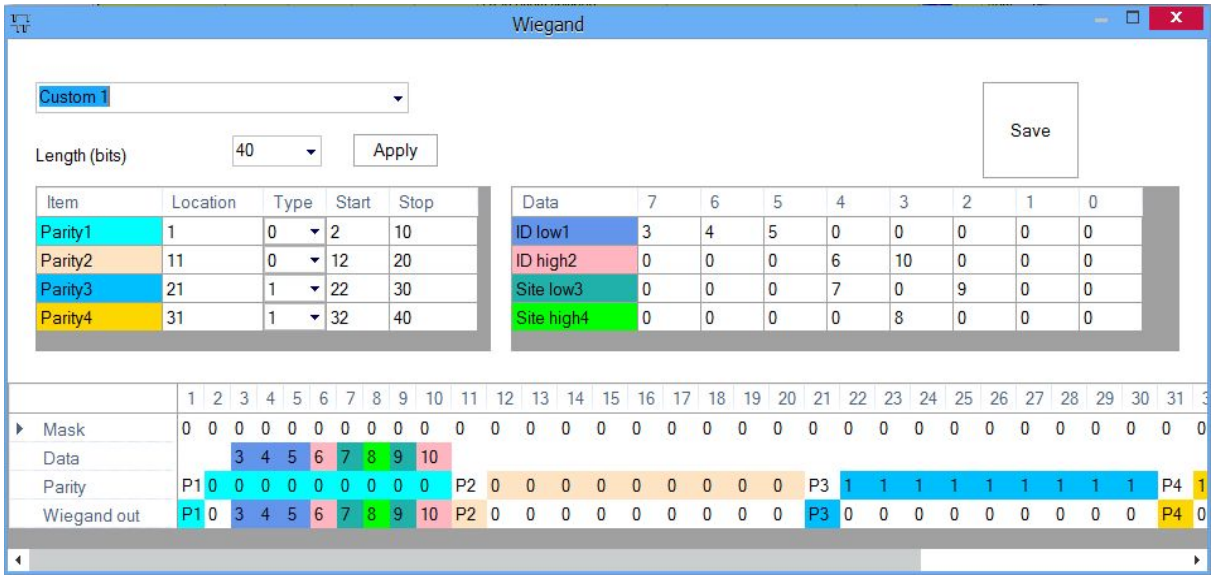
Shadow style

The shadow style can be selected from the menu **View>Appearance>Shadow style**

Wiegand configuration

Select **Settings > Wiegand** from the main menu.

- Select the Wiegand format from the drop-down menu.
    - PROS CS has defined Wiegand 26 and 34 bit as standard options; 3 Wiegand settings remain user definable.
- Set the Wiegand parameters.

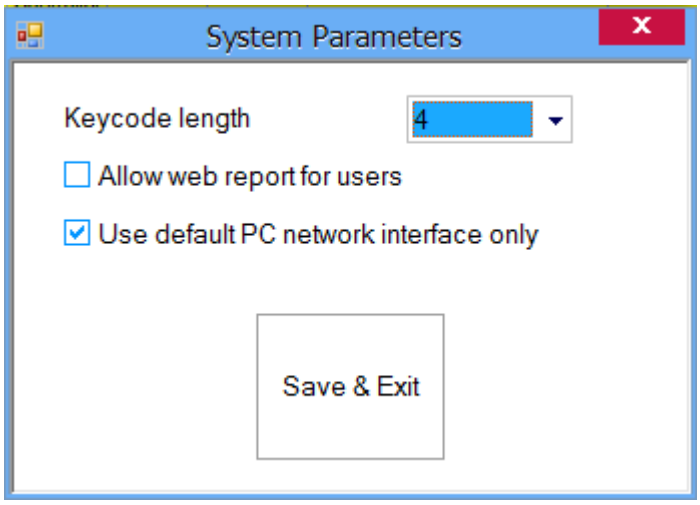

Wiegand
Custom 1
Length (bits)
40
Apply
Save
Item Location Type Start Stop
Parity1 1 0 2 10
Parity2 11 0 12 20
Parity3 21 1 22 30
Parity4 31 1 32 40
Data 7 6 5 4 3 2 1 0
ID low1 3 4 5 0 0 0 0 0
ID high2 0 0 0 6 10 0 0 0
Site low3 0 0 0 7 0 9 0 0
Site high4 0 0 0 0 8 0 0 0
Mask
Data
Parity
Wiegand out

- Click Save to save the settings.

Note: Wiegand settings are not accessible to common end users. Please ask your installer to set the parameters and do not change them later. configuration

System parameters

Select **Settings>System parameters** from the main menu



Keycode length: Defines the number of digits used for a keyed-in code, if the installed hardware supports Code access. This value is valid for all equipment. If entered values for the Keycode are longer than the selected value, digits will be removed from left to right. For example, if the Keycode was 12345678 and the Keycode was reduced to a length of 5 digits, the new Keycode sent to the equipment would be 45678. If the length was increased, the necessary number of zero (0) digits would be added to the left side of the Keycode so that the required length is achieved. If the Keycode has a value of zero (0), it will be considered as "no Keycode".

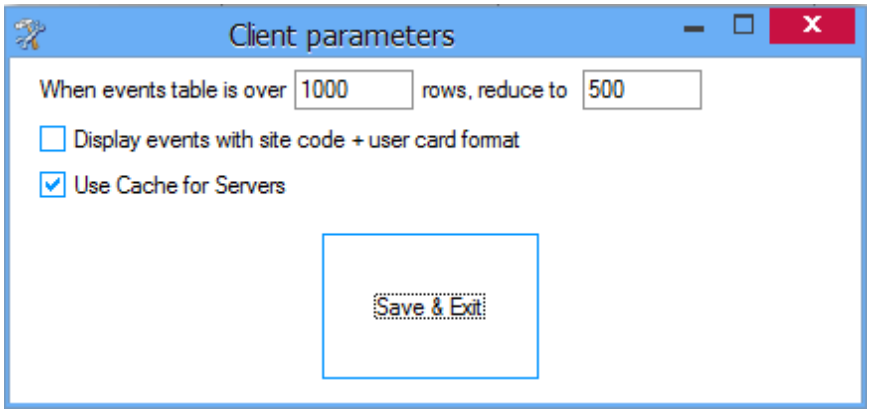
Allow web report for users: If this option is enabled, all users can take a report of their own access

activities using the web report server. Users can access the web server with his or her name and a web password that was entered in Personal Details.

Use default PC network interface only: Use this option if the system is connected to something other than the default network interface in PC.

Client Parameters

Select **Settings>Client parameters** from the main menu



Events display control: The events table contains images that can use up a large amount of system memory and reduce system performance. Therefore when the events table reaches a pre-defined maximum number of events shown, the row number will be reduced to the latest defined number of events.

Display events with Site code + User card format: If this is checked the events table instead of the User's ID it will give the Site code and the User code.

Use Cache for Servers: Use this option for faster logon. If you face any problems while connecting to the server - disable it.

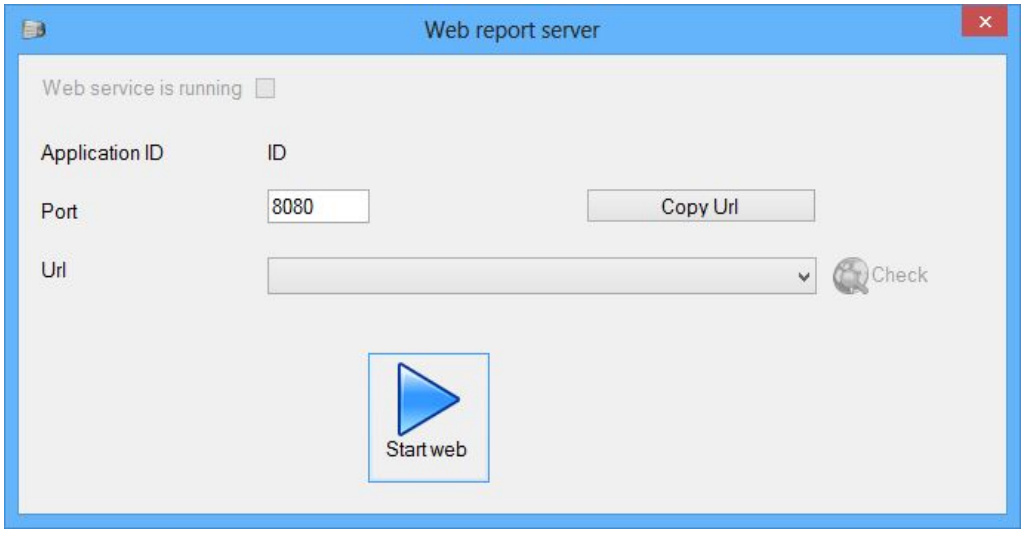
Note: These settings are saved locally in the client, they are not saved in the Server.

Web server

Note: This option is available only if the Client is installed on the same PC as the Server

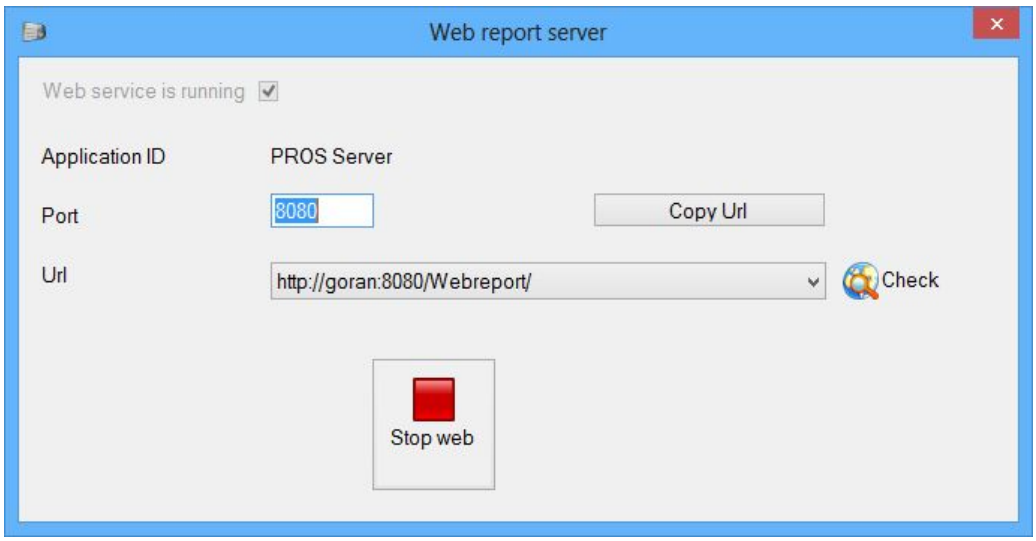
Start/Stop web server

- Select **Settings > Web Service** from the main menu.



- Port: set the web page port number.

- Click the **Start web** button to start the server .



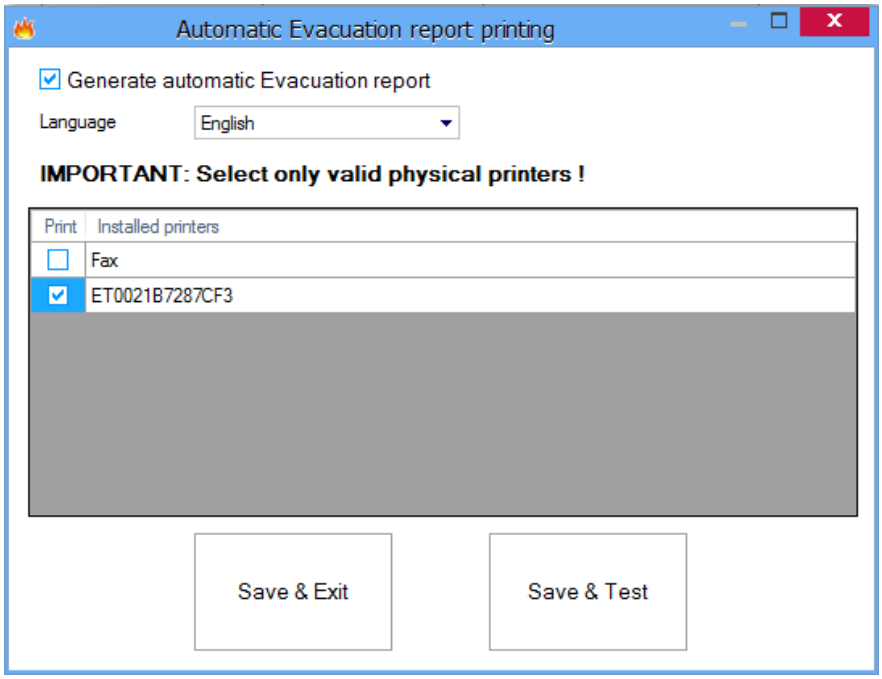
After starting the web server the program will give you the Application ID and the URL for the web.

- Url: gives you a list of the possible links for access via the internet.

- If the service cannot be started, try with a different web page Port value
- Click the **Check** button to open the selected link.
- Click the **Copy Url** button to copy the Url

Automatic Evacuation report printing

- Select **Settings > Automatic Evacuation report printing** from the main menu.



List of installed printers in the Server PC will be shown.

- **Generate automatic Evacuation report -** if enabled, the Server automatically will print Evacuation report in case of a fire on selected printers.
- Select the printers you want the Evacuation report to be printed (**the listed printers are the one installed on the Server's PC**) and click
    - **Save & Test** - to save your configuration and to test the Evacuation report. An Evacuation report should print on the selected printers.
    - **Save & Exit -** to save your configuration.

Scheduled tasks

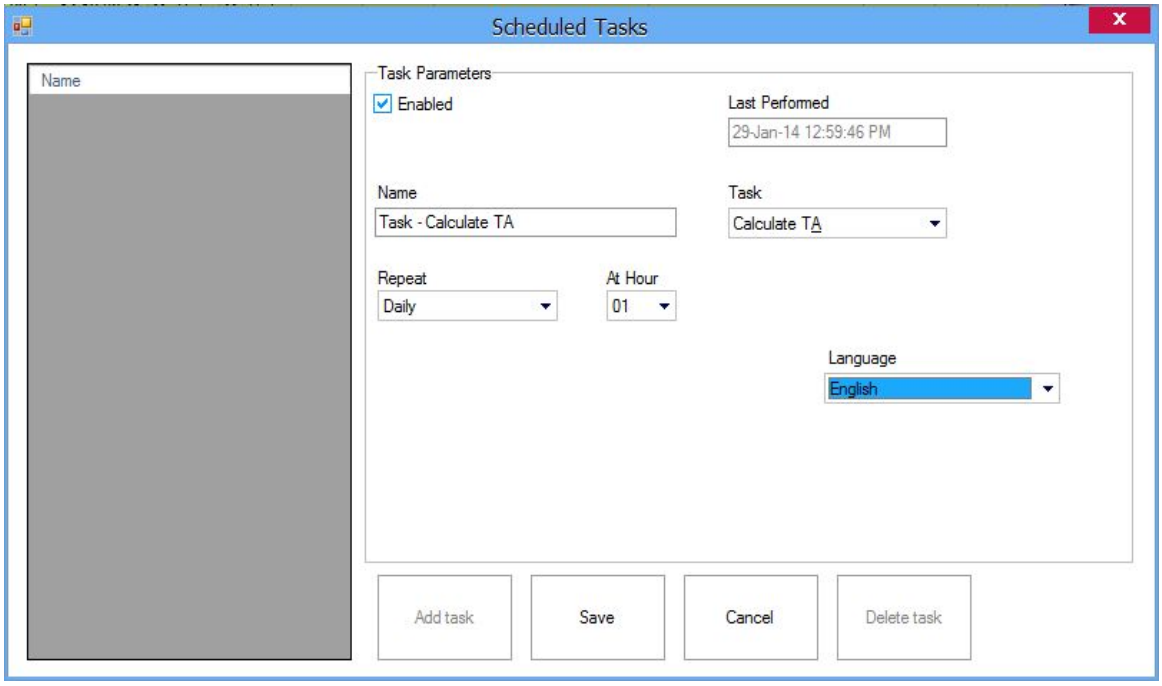
Scheduled tasks are tasks that will be executed by the Server at regular time periods. Periods can be a day, week or month. Each hour from when the Server has started a task routine is performed and all tasks are executed by schedule.

Each task is performed retroactively. The first tasks that are executed are the missing tasks from previous periods.

Example: if Task1 should generate each day at 10:00 hour and the Server was not running for 3 days at the first execution of task routine Task1 it will be executed as running 2 days ago, on the second execution of task routine Task1 (1 hour later) it will be executed as running 1 day ago and then after 1 hour task routine Task1 will be executed as a normal daily task.

1. Adding task

Select **Settings>Scheduled tasks** from the main menu to open the Tasks window



Click the **Add task** button.

The newly created task contains the following parameters:

- **Enable:** If checked the task will be performed otherwise it will be ignored.
- **Last Performed:** Date and time of the last task successful execution. When creating new task **Last Performed = Now.**
- **Name:** The name of the Task
- **Task:**
  a) **Calculate T&A -** calculates T&A data (same as the calculate function in the T&A menu).
  b) **Send by mail -** generate a report and send it by email. In order to be able to send an email the mail account for sending should be set up in the Mail settings window.
  c) **Save to file -** generate a report and save to file.
- **Repeat:**
  a) **Daily**– the task will be executed each day. Calculation and reports will be done for the previous day.
  b) **Weekly**– the task will be executed once a week, the day of the week can be selected in the "At weekday" dropdown list.
  c) **Monthly** – the task will be executed each month on the date selected in the "At day in month" dropdown list.
- **At hour:** select at what period during the day the task will be executed. If 10 is selected the task will be executed in a period between 10:00 and 10:59:59.
- **At weekday:** select a day during the week for the task to be executed. This entry is only available if the task is on a weekly schedule.
- **At day in month:** select a date during the month for the task to be executed. This entry is only available the if task is on monthly schedule.
- **Report:** select one of the saved report templates. Applies for tasks **b** and **c**.
- **File type:** select the report file format for export. Applies for tasks **b** and **c**.
- **Language:** select the Language used when generating the report. Applies for tasks **b** and **c**.
- **Mail to:** type email address of recipients. Applies to task **b**, If more than one recipient is required then separate them by **,** or **;** .
- **Destination:** type in the field or click on button to browse for location where report should be saved. Applies to task c.
- **Test:** Click on this button to check functionality of the task. Applies for tasks b and c after the

task is saved. If the task is correct an email should be sent or a report will be saved.
Click on Save button to save settings.

2. Editing Tasks

Select the task you want to edit. Make the necessary changes and click on the Save button. The changes will be shown after the Server receives them and saves them.

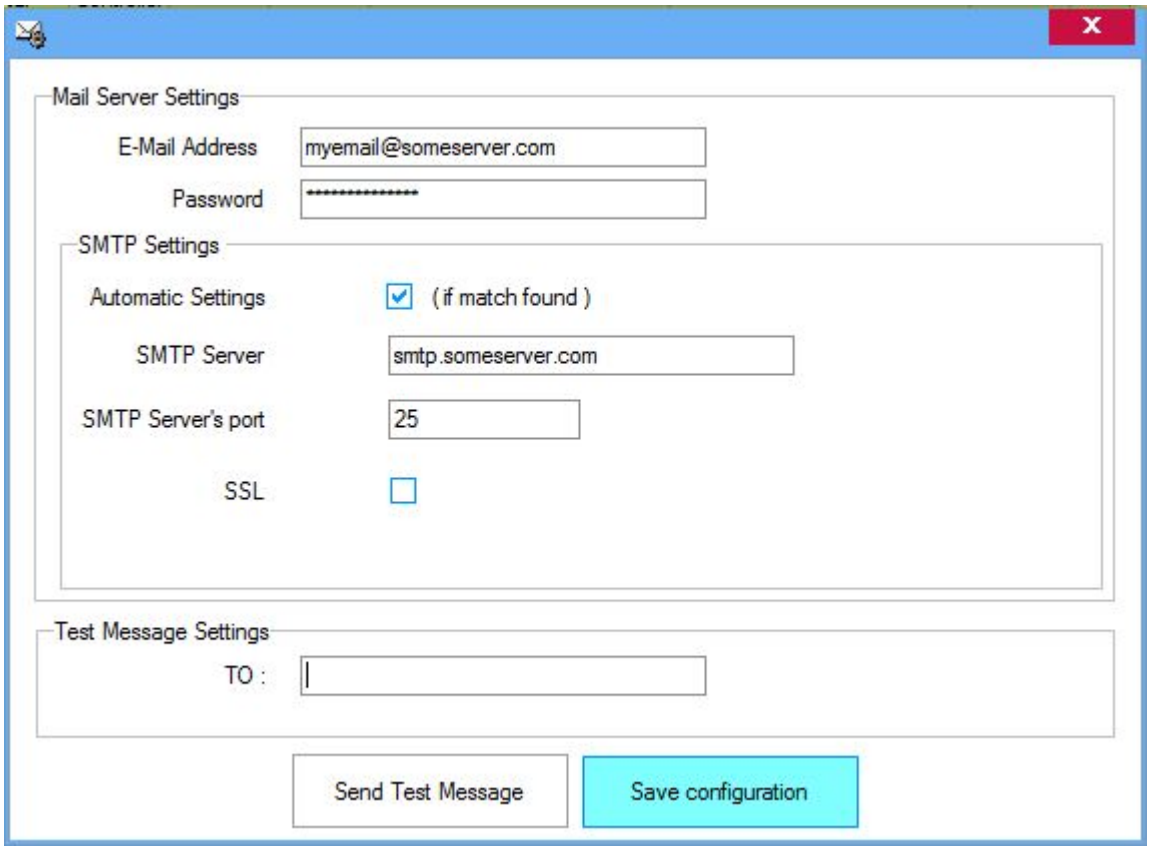
3. Delete Task

Select the task you want to be deleted and click on Delete task button.

Mail settings

Mail settings are email account settings needed for automatic email sending used in Scheduled tasks.

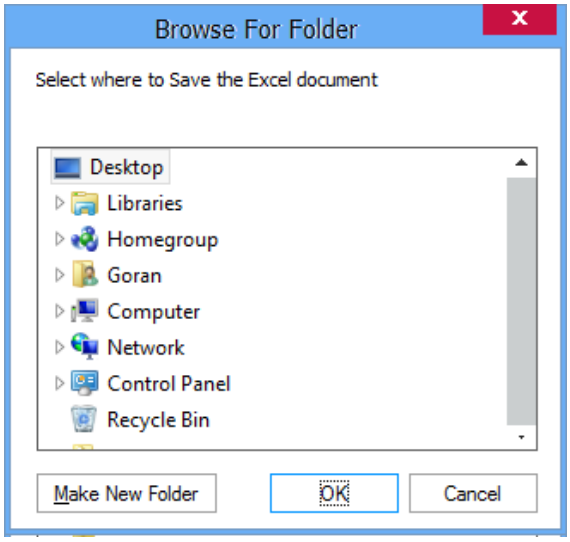
- Select **Settings > Mail settings** from the main menu to open Mail Server Settings window.



- Complete email account details.
- For Test Message Settings type in the recipients email into the **TO** field then click on the Send Test Message button and check if the test message is sent to the correct recipient.
- Click on Save configuration.

Export

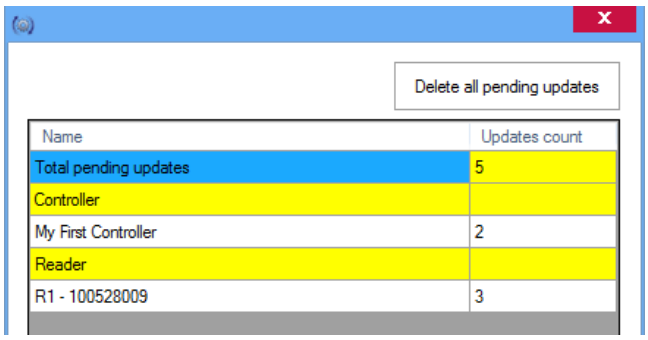
- Select **Settings > Export** from the main menu to export the Users together with all their data to an Excel document
- A windows as the picture bellow will appear. Select the location where you want to save the document and click OK



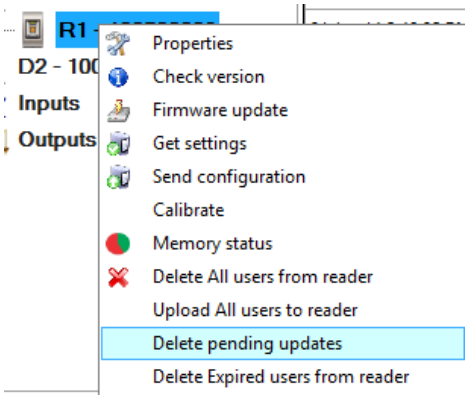
Pending Updates

When a change is made to the software like: new user added, user ID changed, new finger added to the user... - appropriate update is created in the server.
For example: if you have a system with 2 controllers and add new user to the system, 2 updates will be created. First update will be - upload user to controller 1 and second update will be upload user to controller 2. After the updates are finished they are deleted from the Pending updates list. If one of the controllers is offline, the update will be pending until this controller comes back online. Same procedure goes when enrolling finger to a user and save the user. Update is created for each biometry reader according to the access level, or for All biometry readers if user's Access Level = "Unlimited".
If some controller or reader is no longer in the system but it is not deleted from the software, you should check if there are still pending updates for this device and delete them.

- Select **Settings > Pending Updates** from the main menu
- List of pending updates will be displayed



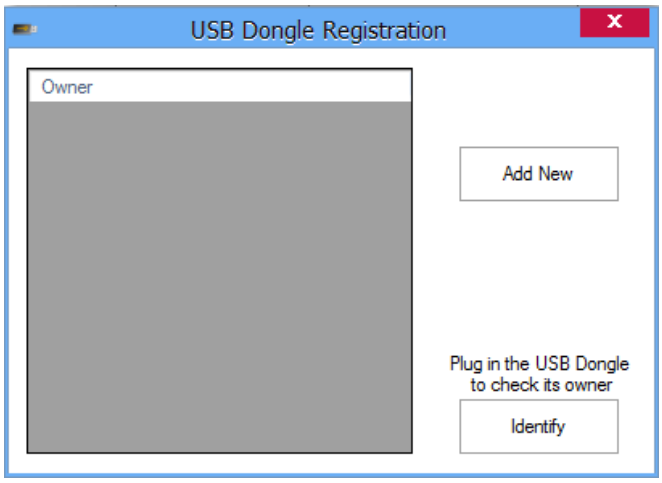
- Deleting pending updates can be done in 2 ways
  - Click on the button "Delete all pending updates" in the window - this will delete ALL pending updates for ALL Controllers and ALL Readers
  - right click on the Reader/Controller and then select "Delete pending updates" - this will delete ALL pending updates ONLY for that Reader/Controller



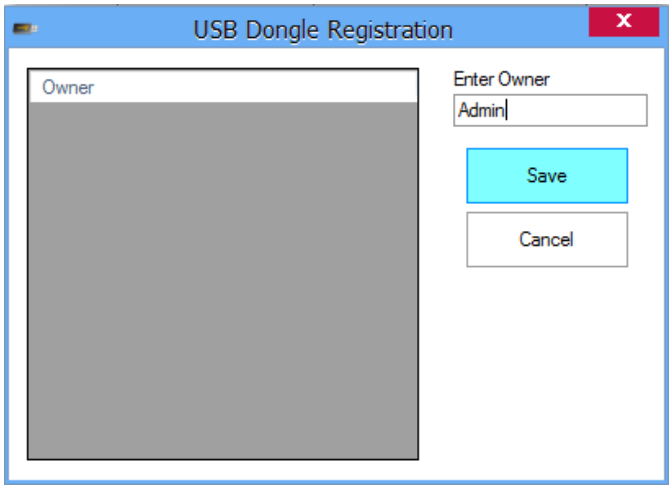
USB Dongle Registration

Note: This menu is only available with Admin login

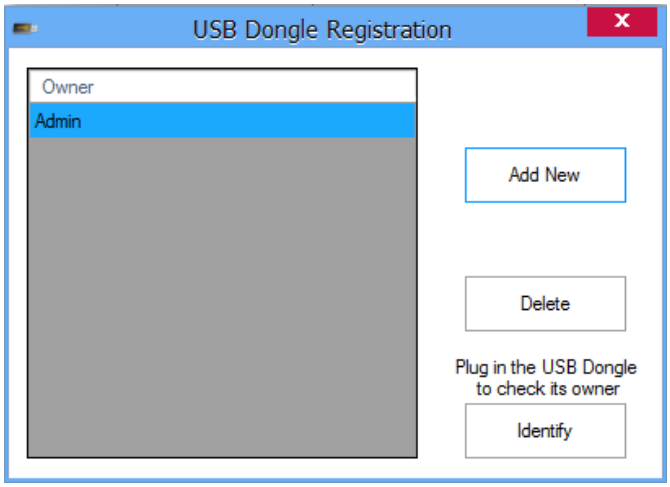
- Select **Settings > USB Dongle Registration** from the main menu
- The USB Dongle is used when connecting to a Server on a remote PC (Client and Server are not on the same PC)
- First you need to register the USB Dongle at the Server.
    - Start the Client that is on the same PC as the Server
    - open USB Dongle Registration window



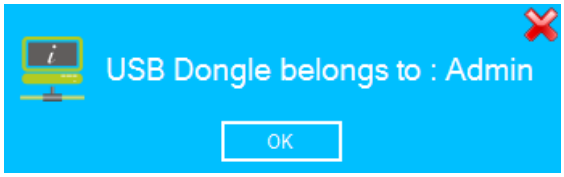
    - insert the USB Dongle into some of the USB ports of the PC
    - click on Add New
    - Enter the name of the Owner that will be using the USB Dongle and click on Save



- New USB Dongle should be added In the list on the left



- If you want to check the Owner of some USB Dongle, insert it into some of the USB ports of the PC and click on Identify. You should get info like the picture bellow.

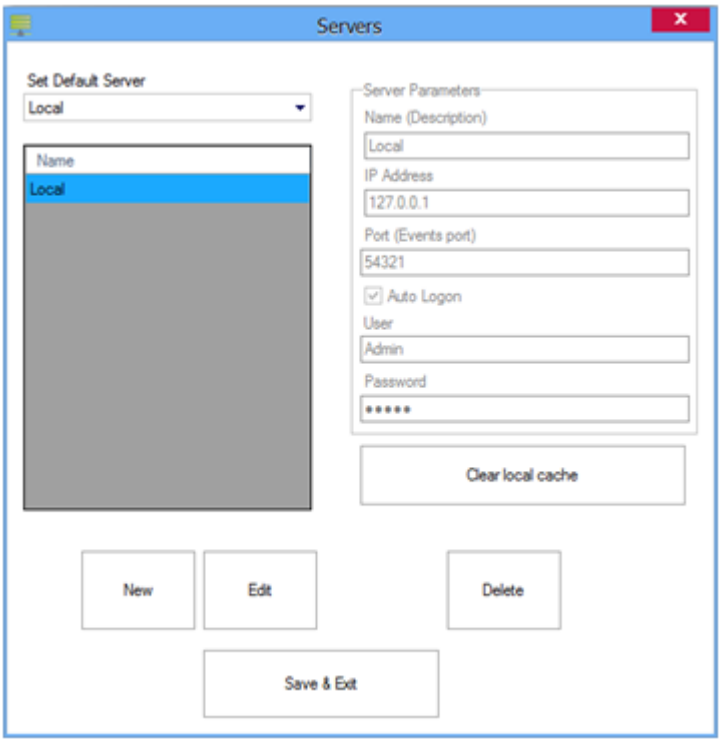


- If you want to delete the USB Dongle from the system - click on it in the list and then click on Delete

Servers

- Select **Settings > Servers** from the main menu

This is where the connection to the server(s) is set. Here you can change or add new Servers. The default server is Local (Local = the Client is on the same PC as the Server). If your Server is on a remote PC (not the same PC as the Client) then you will need to add new Server.



Name: Name of the server

IP Address: IP Address of the Server. If the server is on your local network you just type Server's IP address here, otherwise you will need Server's global IP address and you will need to do port forwarding in the router the server is connected to

Port: the Event port set in the Server Setup. (the Default is 54321)

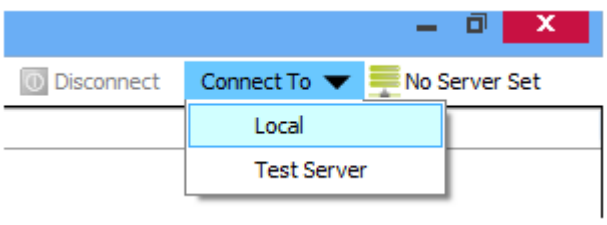
Auto Logon: check if you want the Client to logon automatically to the Server

User: Name of the Operator connecting to the Server(see Operators). Enabled if Auto Logon checked

Password: Operator password (see Operators). Enabled if Auto Logon checked

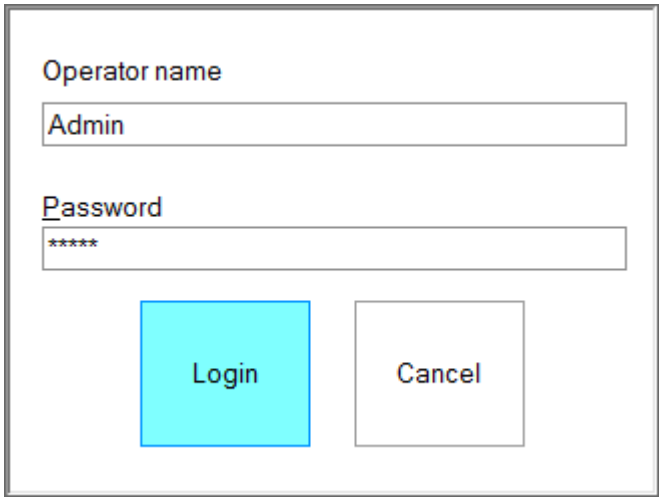
Clear local cache: Client keeps local cache for each Server in order to speed up the connecting procedure with the server (necessary data for client to run is taken from the Server only once, and each next connection takes only the new changes made)

After configuring the Servers, you can choose a Server from the “Connect To” menu in the top-right corner of the Client. You can connect to other Server without closing the Client by clicking the Disconnect button and then choose a server in the dropdown list. If you want to see info about the current server, just click on the icon next to the “Connect To” menu and an info window will be displayed onscreen.



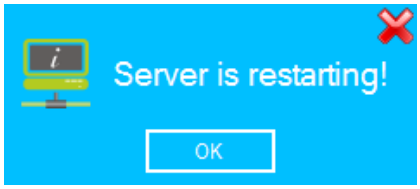
If "Auto Logon" is not checked for the current server, when connecting a login window appears onscreen

asking for credentials. (The default setting is Operator name = "Admin" and Password = "admin")



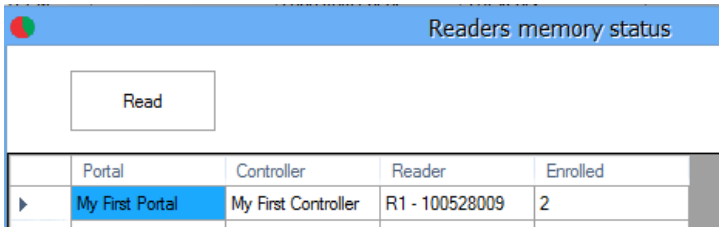
Restart Server

- Select **Settings > Restart Server** from the main menu
- After the Server receives the command for Restarting, it sends the following message to all Clients and then Restarts.

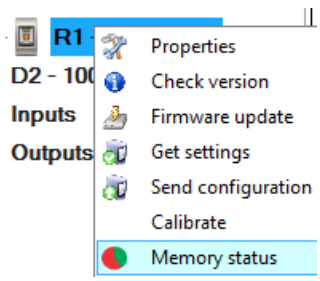


Memory Status of Biometry Readers

- Select **Biometry > Memory Status** from the main menu
- Click on Read. List of all biometry readers will be shown with the number of enrolled fingers per each reader



- If you want to check Memory status for a specific reader, right-click on the reader and select "Memory status".



- The following event will be shown in the events table

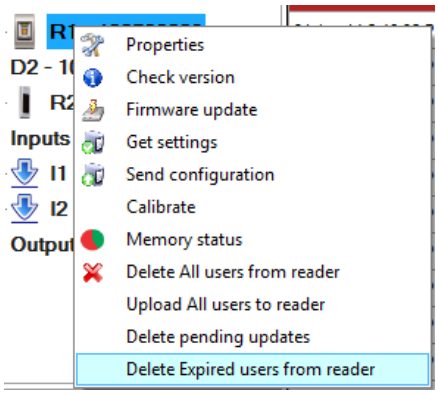
Time	Portal	Controller	Reader	Door	Event
31-Jan-14 4:22:01 PM	My First Portal	My First Controller	R1 - 100528009		Enrolled fingers : 2

Delete Expired Users from all Biometry Readers

- Select **Biometry > Delete expired users from all readers** from the main menu
- This will delete ALL expired users from ALL biometry Readers (**Valid to** date parameter of the user is less than today)
- The following event will be shown in the events table

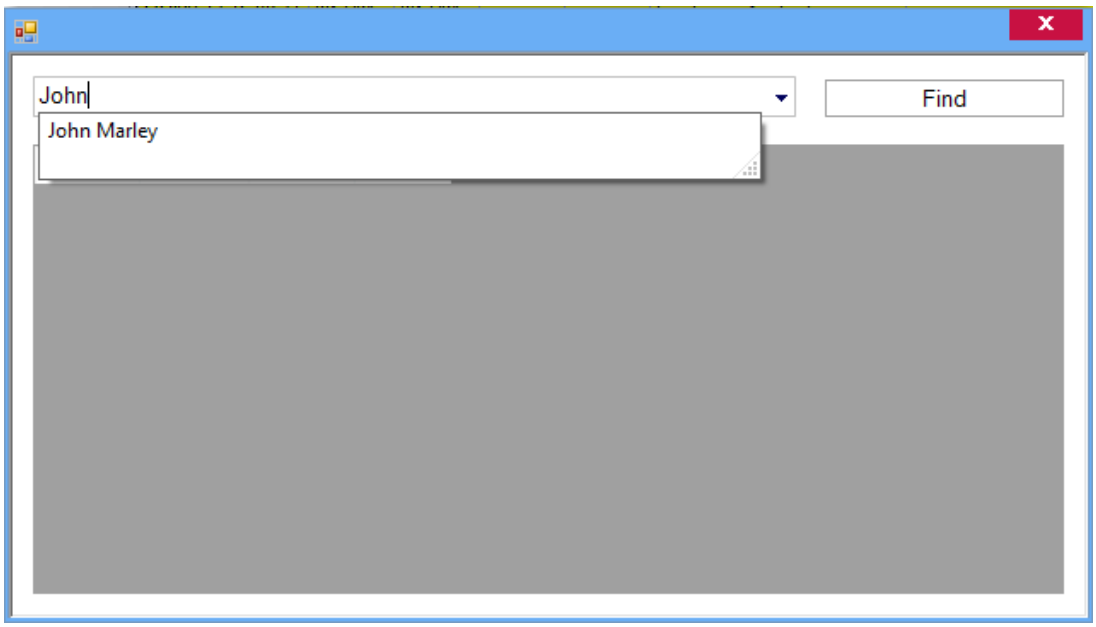
Time	Portal	Controller	Reader	Door	Event	User
31-Jan-14 4:07:05 PM			R1 - 100528009		Sucessfully added task	Delete expired users

- If you want to delete the expired users only from a specific biometry reader, right-click on the reader and select "Delete expired users from reader"



Find users

- Select **Find > User** from the main menu.



- Type or select the name of the user in the drop-down list and click Find.
    - The search will show all the users whose names contain the string written in the drop-down box.

Hardware settings

Portals

What is a portal?

A Portal is a communication link between the Server and the devices in the system. A Portal has two parts - logical, recognizable by the software, and physically – an electronic device connected to a computer and other devices in the system known as converters.

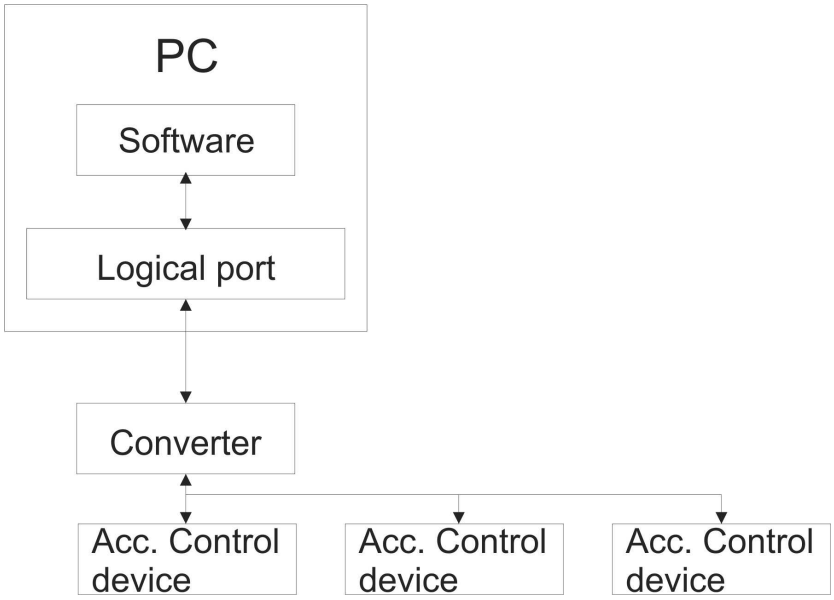
The Logical part can be:

1. Serial port (COM)
2. Network port

The Physical part can be:

1. RS232 to RS485 converter, connected to a logical Serial port
2. USB to RS485 converter, connected to a logical Serial port
3. TCP/IP to RS485 converter, connected to a logical Network port

The Server can use more than one portal to connect to devices in the system. Devices in the system can be connected to the Server, with one portal only. Only one Serial portal can be used in the Server.



Hardware

RS232 to RS485

This converter is connected to the PC's COM port. It is powered by the COM port so it does not require a

separate power supply, except in the case that the PC's COM port does not have all its signal outputs used for power (DTR, RTS) or enough power to drive the converter. This converter does not require any drivers to be installed if the COM port on the PC side is installed properly.

Requirements:

- Available PC COM port (RS232)
- RS232 to RS485 converter

USB to RS485

This converter is connected to the PC's USB port. It is powered by the USB port so it does not require a separate power supply, except in the case that the PC's USB port does not have enough power to drive a converter. This converter needs the suitable driver to be installed before use. If installed using the PC's driver manager it will appear as a COM port.

Requirements:

- Available PC USB port
- USB to RS485 converter

TCP/IP to RS485

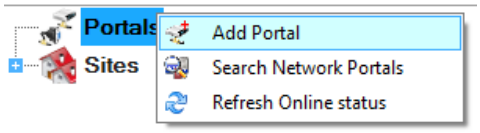
This converter is connected to the PC over a local network or directly with a network patch cable. It uses an external power supply. This converter does not need any drivers to be installed. Some Access control equipment may have a built-in TCP converter used by the same device and other devices in the system to communicate with the Server.

Requirements:

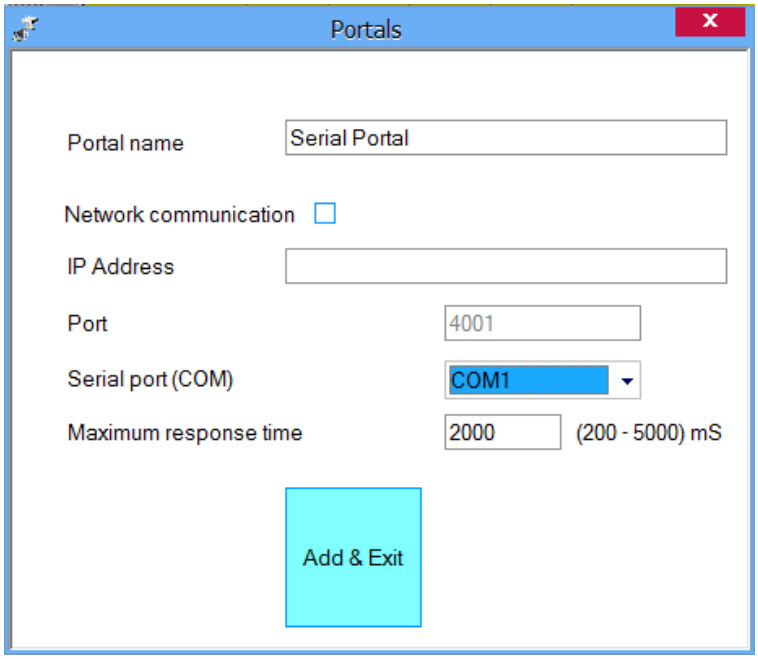
- Access to local network or PC network card.
- TCP/IP to RS485 converter

Add a Serial Portal

- Right-click on the **Portals** item and select "Add portal"



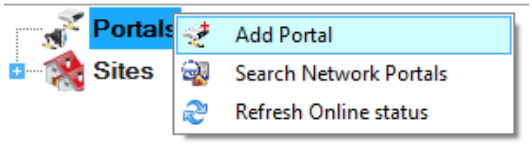
- Enter the portal name
- Make sure that the Network communication option is not checked
- Select the COM port from the Serial port drop-down list (COM ports on the Server PC)



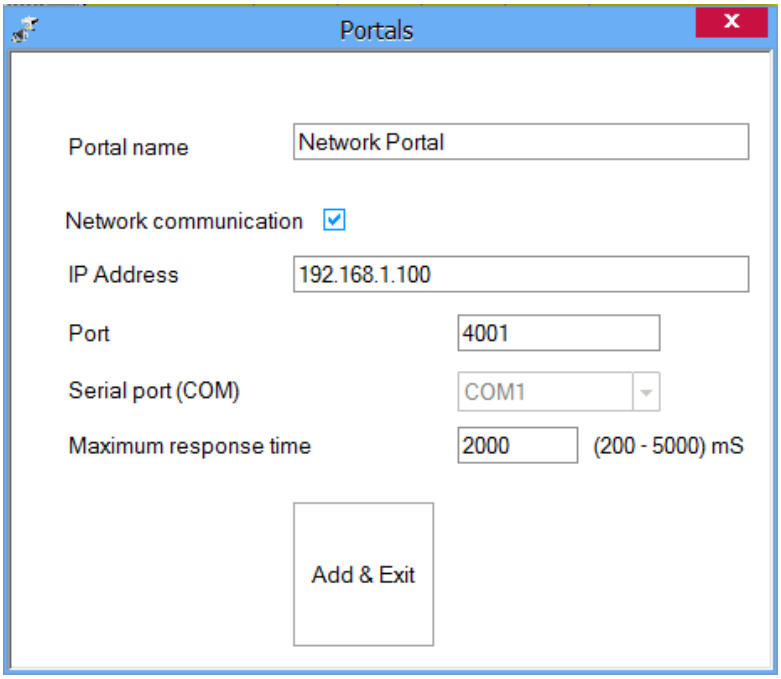
- Click on **Add & Exit**
- The New portal is shown below the Portals item with a given name and a picture of the serial portal

Add a Network portal

- Right-click on the **Portals** item and select "Add portal"



- Check the Network communication option
- Consult your installer for the portal's IP address and Port, and fill in the Portal properties window with the data.

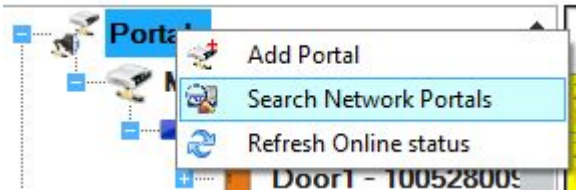


- Click on **Add & Exit**
- The new portal is shown below the Portals item with a given name and a picture of the network portal

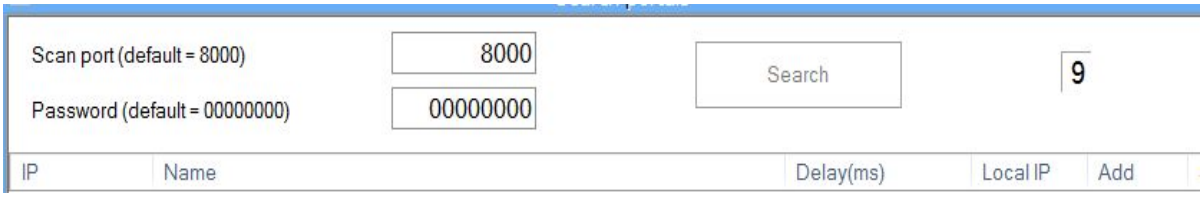
Search network portals

This procedure is valid only if you have EWSi connected to the network

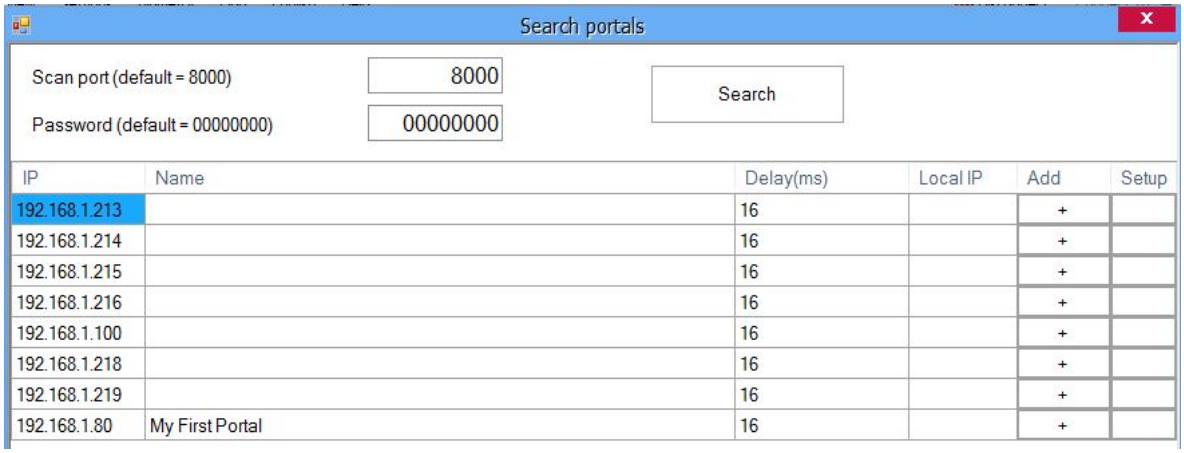
- Right-click on the Portals icon and select the Search network portals



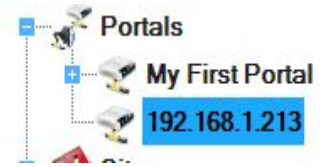
- On the Search portal window select the port to search (default is 8000)
- Click on the Search button and wait



- If any portal is found, it will be displayed in the table

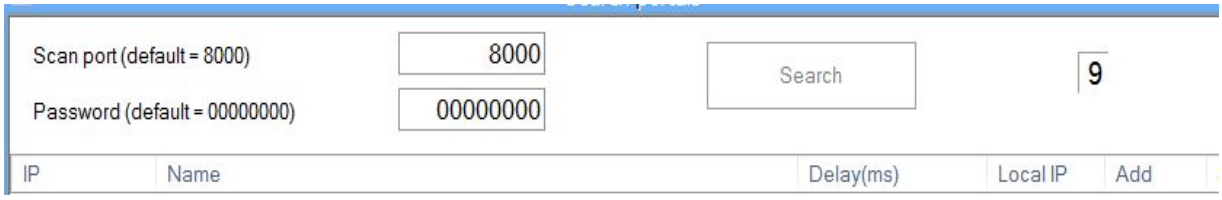


- If the Portal does not exist in the Server click on the Add column button in the portal row.
- The Portal will be added to your collection of Portals with the same name as the found device IP

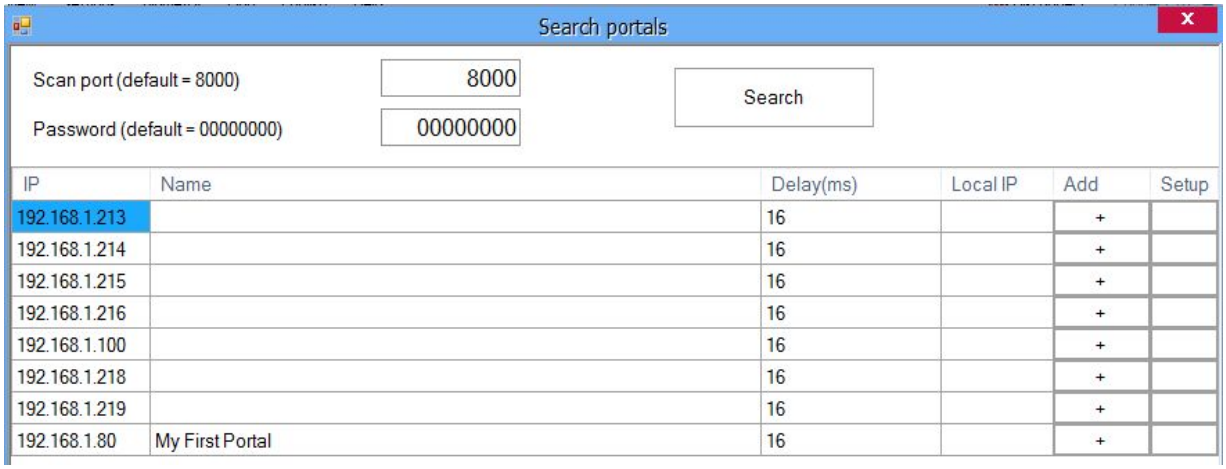


Configure the portal

- Right-click on the Portals icon and select the Search network portals
- On the Search portal window select the port to search (the default is 8000)
- Click on the Search button and wait

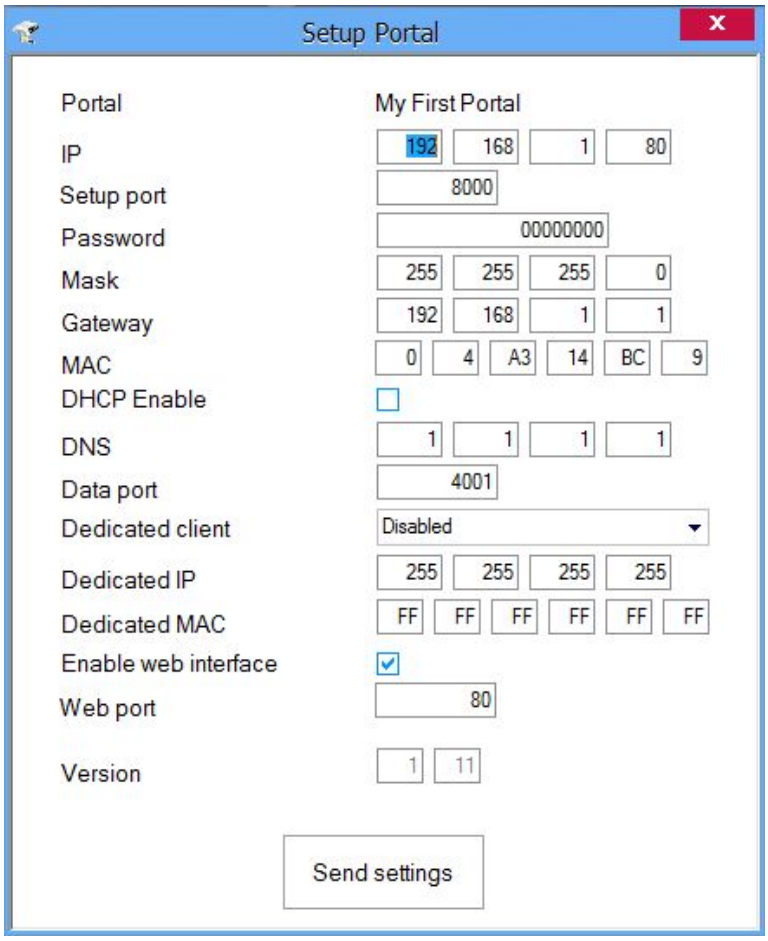


- If any portal is found, it will be displayed in the table



- Enter an 8 digit device password (factory default is 00000000)
- Find a row with a portal to configure and click on the appropriate Setup button. The following window will be shown

- After the server executes the request the setup portal window will be shown with the portal settings. If the values are empty, reading settings from CNV1000 will not be possible



- Enter new settings:
  - **IP:** IP address of device
  - **Setup port:** Network port for search and setup. Changing is not recommended
  - **Password:** Password for access to read and change the settings of the CNV1000. It is recommended to change the default password and use it for all converters in the system.
  - **Mask:** Enter the device subnet mask
  - **Gateway:** Default gateway
  - **MAC:** Physical address of the device. Changing is not recommended

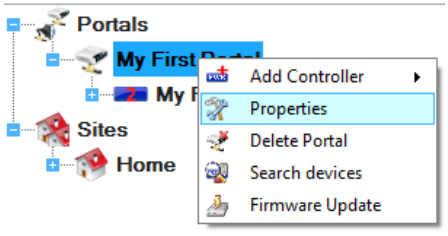
- **DHCP Enable:** Enable the DHCP client
- **DNS:** Address of the DNS server
- **Data port:** Port used for communication between the Server and devices behind the converter
- **Dedicated client:** To forbid unauthorized access to devices connected to the portal from another system, select one of the following options
  a) **Disabled** - no source security checking
  b) **MAC only** - the source MAC address must be equal to the Dedicated MAC value
  c) **IP only**– the source IP address must be equal to the Dedicated IP value
  d) **IP or MAC** - at least one of the conditions from point b and c must be true
  e) **IP and MAC** - both b and c conditions must be true
- **Enable web interface:** enable or disable the CNV1000 web interface for configuration
- **Web port:** Web interface port
- **Version:** Read-only field displaying the firmware version of the converter

- Click on Send settings to configure the device. After the server sends the settings the following will be shown in the event window

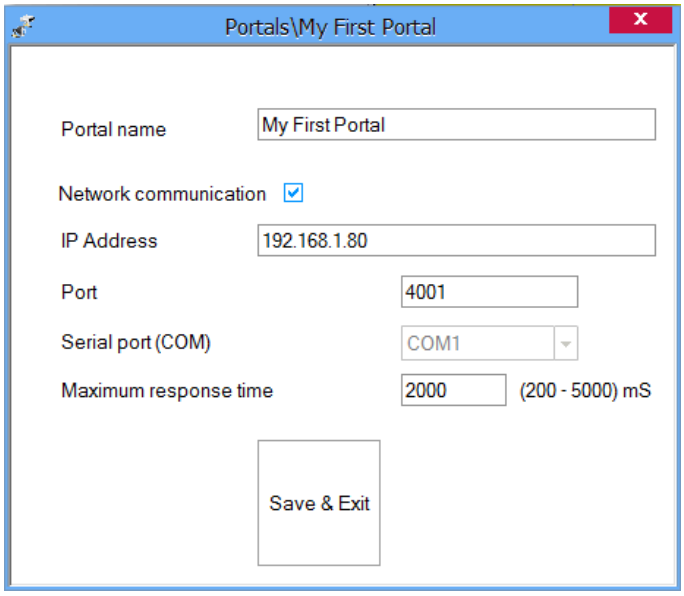
Time	Portal	Controller	Reader	Door	Event
29-Jan-14 3:56:53 PM					Setup Portal : Service setup done.

Edit a portal

- Right-click on portal and select Properties



- Change the settings on the properties window

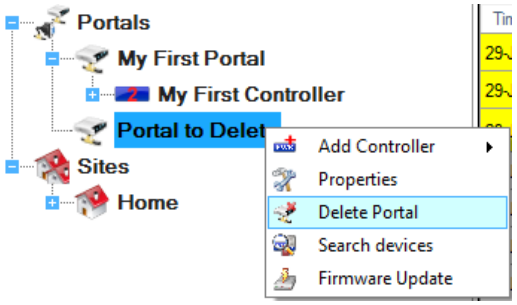


- Click on the Save & Exit button

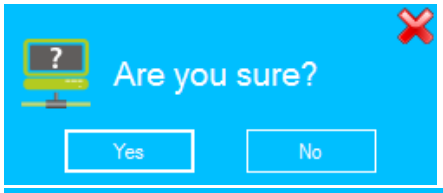
Delete a portal

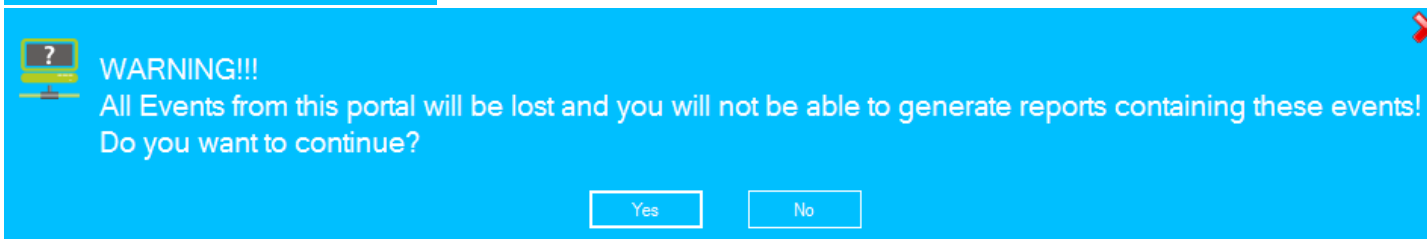
The Portal can be deleted only if there is no device added to it

- Right-click on the portal and select the Delete menu



- Confirm deletion

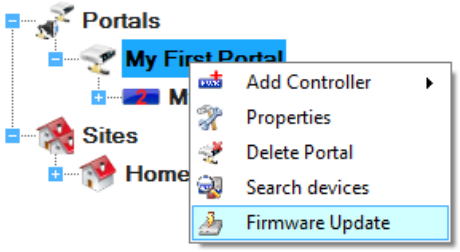



WARNING!!!
All Events from this portal will be lost and you will not be able to generate reports containing these events!
Do you want to continue?
Yes
No

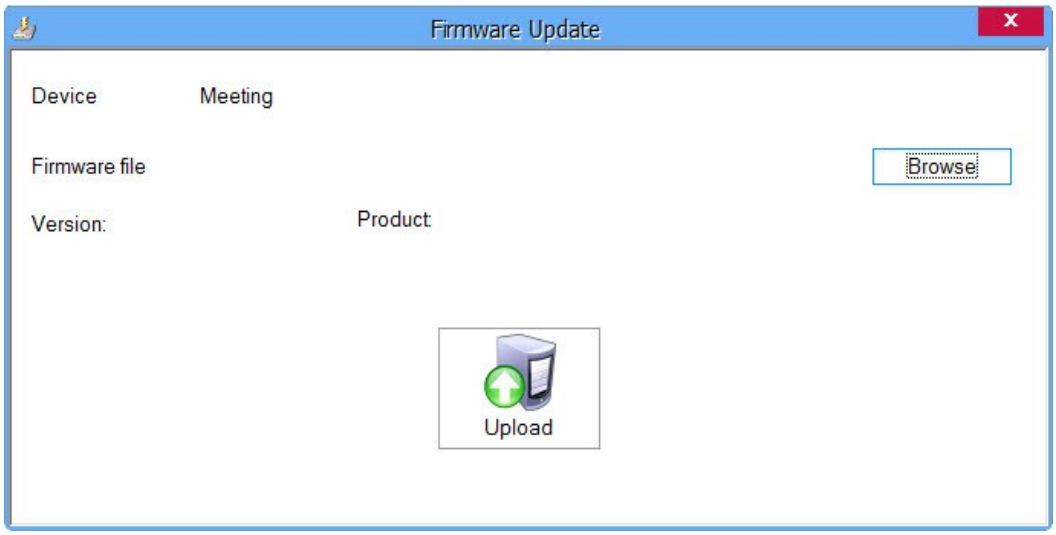
Firmware update

A Firmware update can only be done to a CNV1000 standalone or embedded converter

- Check the portal firmware version by using the Configure CNV1000 procedure
- Right-click on the portal to be updated and select the Firmware update menu



- On the Firmware update window, click the Browse button. The default location of the firmware files installed with PROS CS Setup is in the Client installation folder under "Firmware" folder. If you have a newer version, use browse to locate it.
- Select the firmware file with a "xhc" extension
- Check the firmware version. If the version is not greater than the existing version of the CNV1000 then do not upgrade with this file, unless specified by the installer or manufacturer of this device.



- Click on the Upload button. After the server starts the update you should receive the following event

29-Jan-14 4:06:24 PM	My First Portal				Firmware update started

- After the server finishes the update you should receive the following event

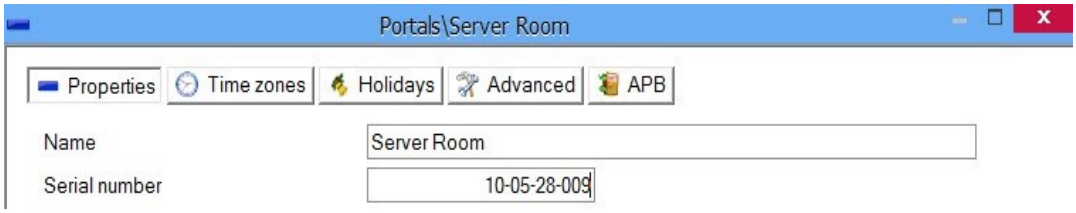
29-Jan-14 4:06:48 PM	My First Portal				Firmware update success

Control panels

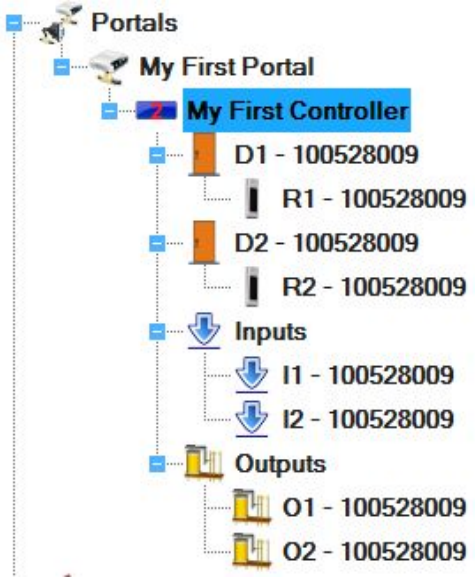
Add a controller

- Right-click on a portal connected to the controller and select **Add controller>EWS**

- Enter Name and Serial number of the controller. The Serial number is provided on the controller's board.



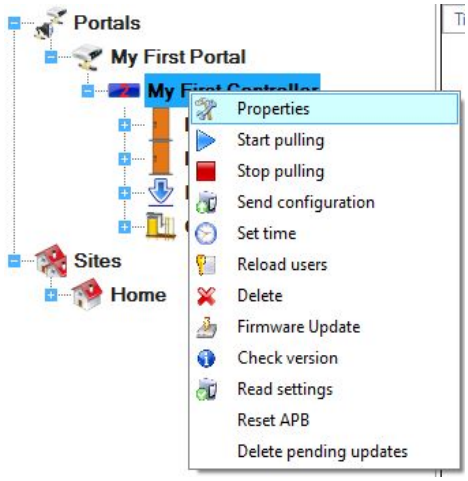
- Click on the Save and Exit button
- The New controller and the controller peripherals are shown under the portal item



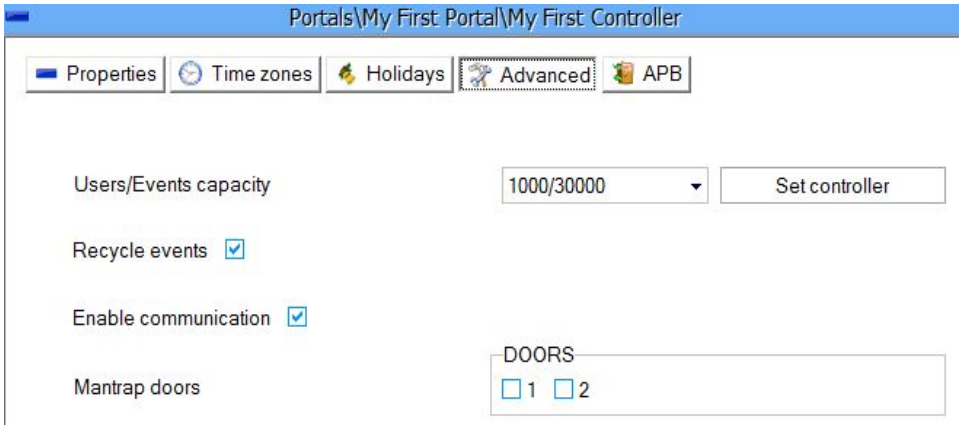
- In order to see if EWS is online and communicating with the PC, right click on the Controller and select "Check Version" from the controller drop-down menu. In the event panel it will be indicated if the controller is on line or not. If the Serial Number does not match, the controller will not go on line. If there is no communication, the controller name will have a red background color in the tree view.

Edit a controller

- Right-click on the controller and select the Properties menu



- On the controller properties window select the Advanced tab



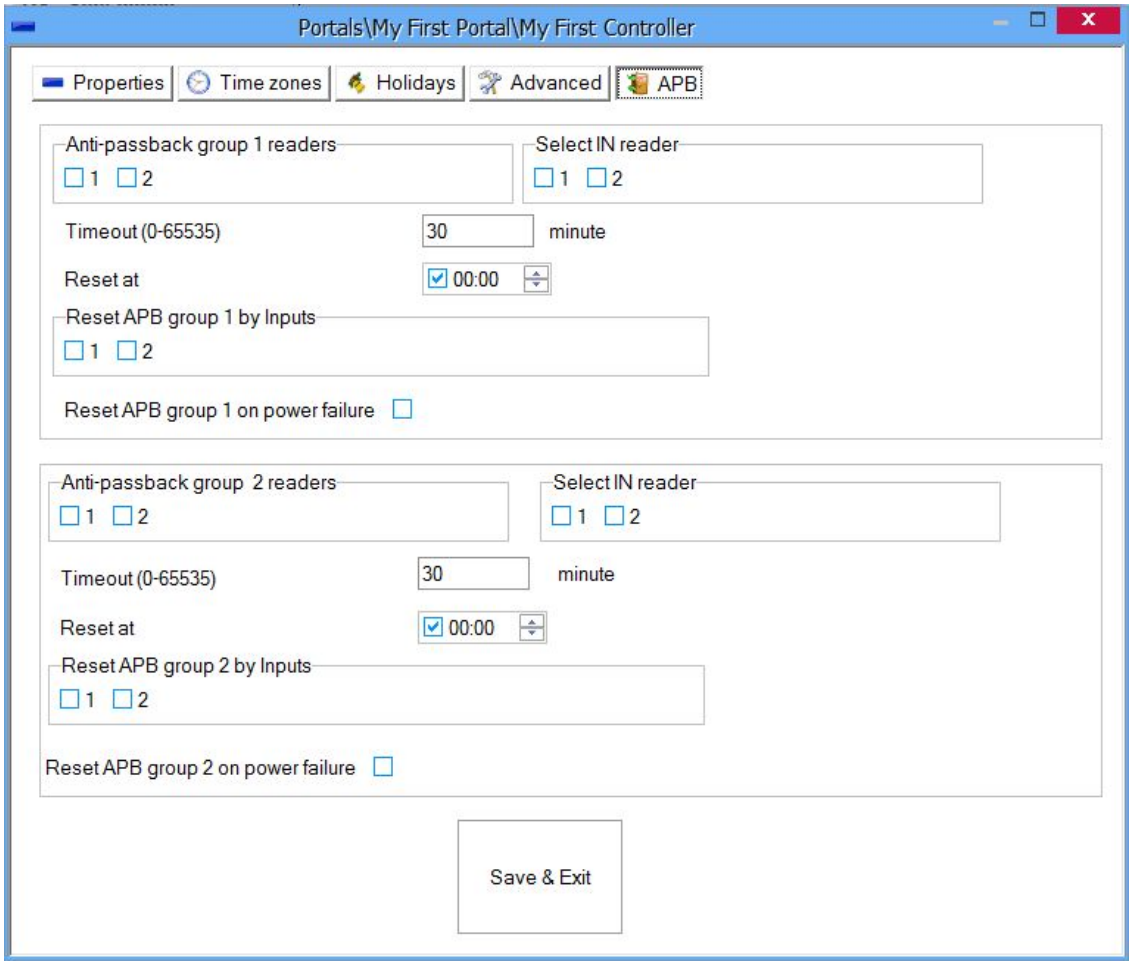
- **Users/Events capacity**: This option allows to change the capacity of the EWS. More Users = Less Events capacity and vice versa.

- **Recycle events**: When option is checked then the EWS will delete the events from its memory when it is full.

- **Enable communication:** If the Enable communication is not checked,when the Server is started, the event pooling from the controller will not run until it is started manually via the controller menu option "Start pooling"

- **Mantrap doors:** If the mantrap option is used,check the doors to be used in the mantrap

- Select APB tab (anti-passback)



- Configure two Anti-passback reader groups if required

- **Anti-passback group readers:** select the readers in the APB group

- **Select IN reader:** Select the readers allowing entry to the protected area in the APB group. The selected readers must also be selected in the Anti-passback group readers.

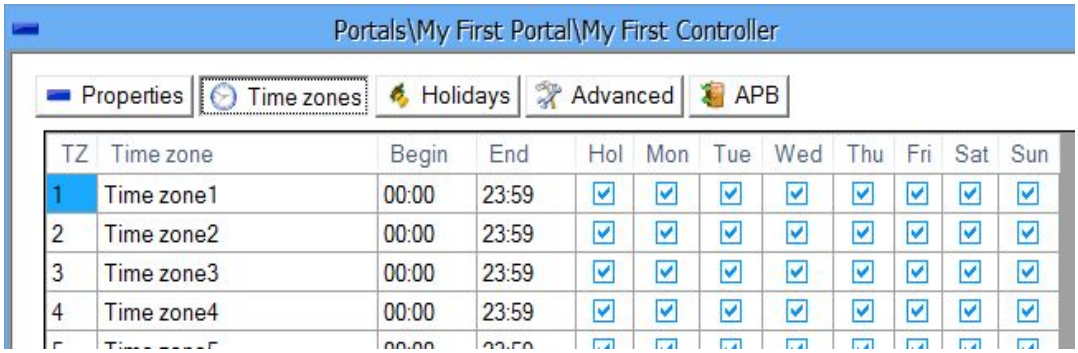
- **Timeout:** Set the time period, in minutes, required to allow the user to enter the protected area again without exiting the same area. If this option is not required, enter 0.

- **Reset at:** The time of the day for the APB options to be reset. All users will be considered as out of the protected area.

- **Reset APB by Inputs:** Assign Inputs to reset APB.

- **Reset APB on power failure:**APB status will be reset whenever the EWS controller is powered down and then powered back up again (power switched back ON).

- Select Time Zones tab.


Portals\My First Portal\My First Controller
Properties
Time zones
Holidays
Advanced
APB
TZ Time zone Begin End Hol Mon Tue Wed Thu Fri Sat Sun
1 Time zone1 00:00 23:59
2 Time zone2 00:00 23:59
3 Time zone3 00:00 23:59
4 Time zone4 00:00 23:59

- Set the time zone per controller.

Time zones are time periods with validity defined by a start and stop time in a day. The total number of time zones is 24. Planning the time zones should be done carefully because the same zones are used for access levels, doors, readers and input and output configuration. It is recommended to plan these steps carefully before starting system configuration.

- **Time zone name:** enter the time zone name.

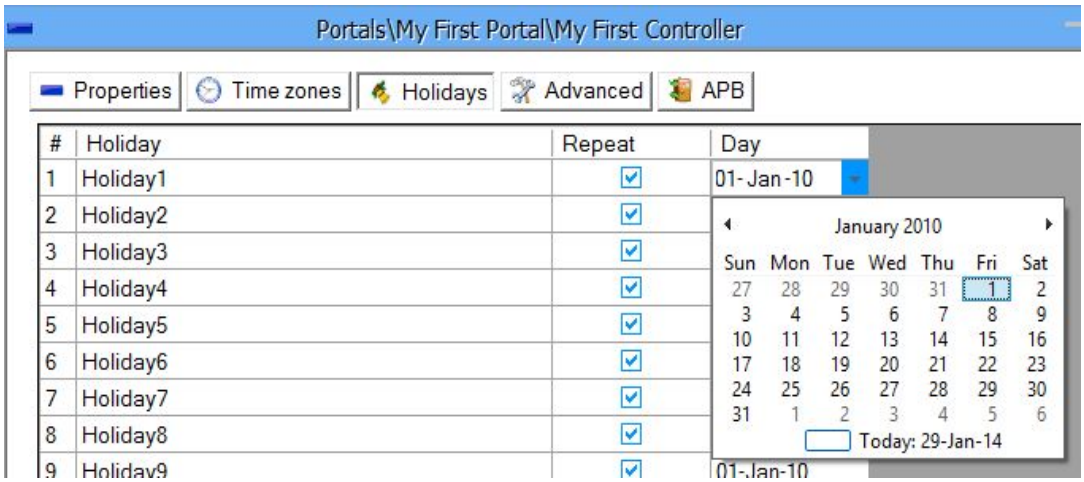
- **Begin:** enter the time zone start time of the day.

- **End:** enter the time zone end time of the day.

- **Hol:** set if the time zone is valid for holidays.

- **Mon-Sun:** set the weekday validity.

- Select Holidays tab.



- Set Holidays per controller.

- **Holiday column:** enter the holiday name.

- **Repeat column:** check to make the holiday valid annually.

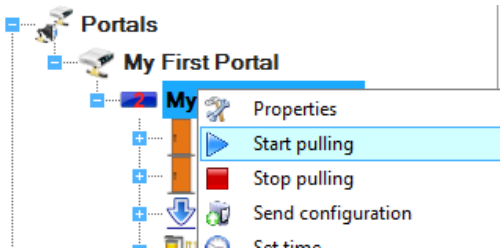
- **Day column:** enter the holiday date or click on the right side and select the date in the new calendar window.

- Click on the Save & Exit button.

- The Server will configure the controller automatically

Start/stop pooling

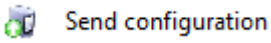
- Right-click on the controller and select the Start or Stop pooling menu



This setting will be valid until the Server is restarted.

Upload configuration to a controller

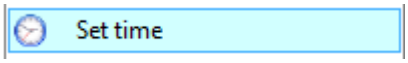
- Right-click on the controller and select the Send configuration menu



- See the events panel to check the configuration flow

Set controller time

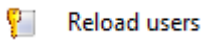
- Right-click on the controller and select the Set time menu



The Time and Date value from the PC will be sent to the controller. Check the PC's time and date accuracy before using this command.

Upload users database

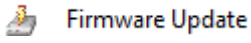
- Right-click on the controller and select the Reload users menu



This command will erase the controller user database and upload users from the PC database

Firmware update

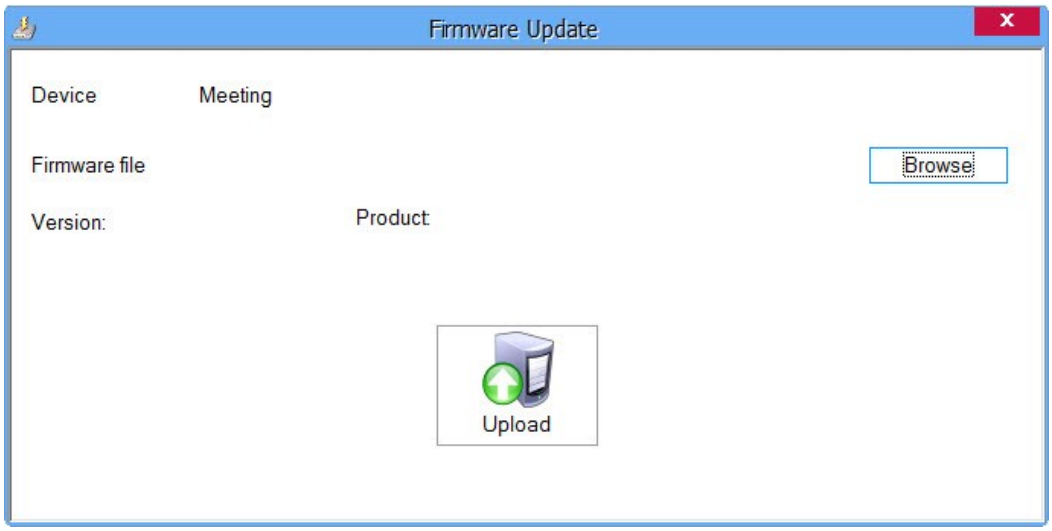
- Check the controller firmware version
- Right-click on the controller and select the Firmware update menu



- On the Firmware update window, click the Browse button. The default location of the firmware files installed with PROS CS setup is in the Client installation folder under "Firmware" folder. If you have a

newer version, use browse to locate it.

- Select the firmware file with an "xhc" extension.
- Check the firmware version. If the version is not greater than the existing version of the controller then do not upgrade with this file unless specified by the installer or manufacturer of this device.



- Click on the Upload button
- After the server starts the update you should receive the following event

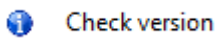
Time	Portal	Controller	Reader	Door	Event
30-Jan-14 9:03:41 AM	My First Portal	My First Controller			Firmware update started

- After the server finishes the update you should receive the following event

Time	Portal	Controller	Reader	Door	Event
30-Jan-14 9:04:28 AM	My First Portal	My First Controller			Firmware update success

Check firmware version

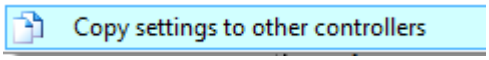
- Right-click on the controller and select the Check version menu



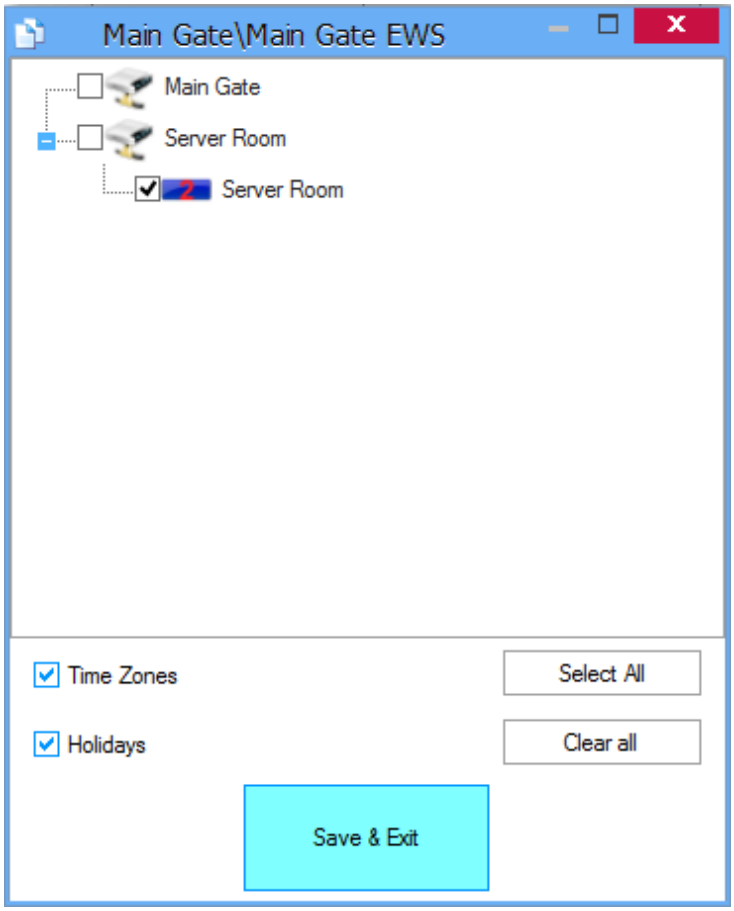
The version is displayed in the events panel

Copy controller settings

- Right-click on the controller and select the "Copy settings to other controllers" menu



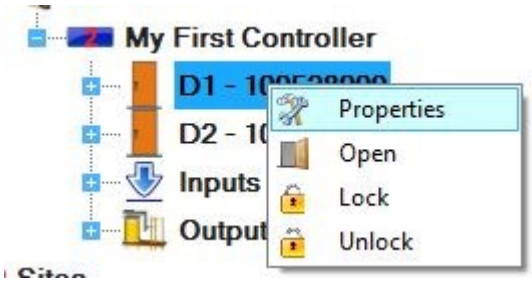
- Choose the controllers that you want to apply current controller settings
  - Check "Time Zones" if you want to copy Time Zones settings
  - Check "Holidays" if you want to copy Holidays settings



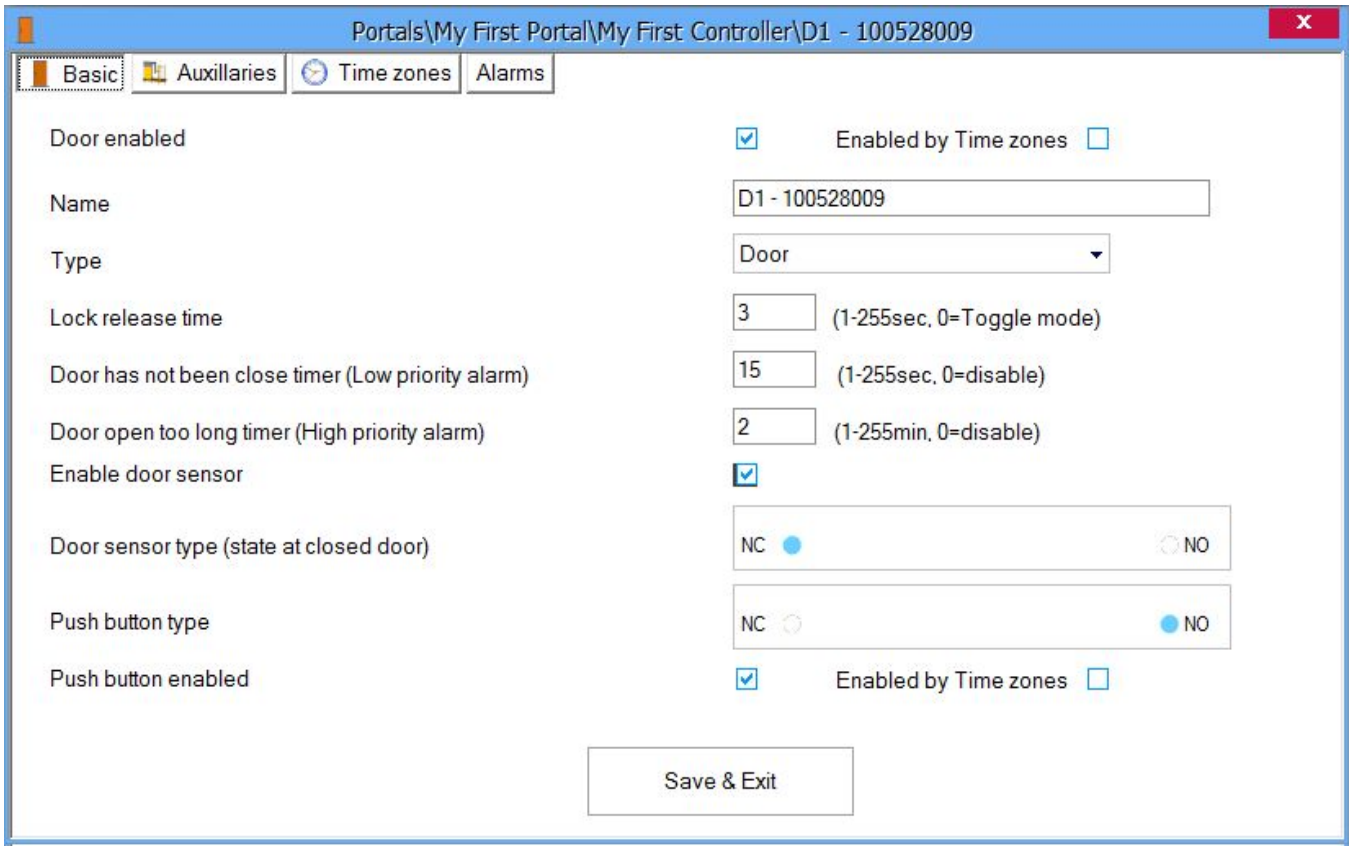
Doors

- Expand the controller item to see the doors

- Right-click on the door to be configured and select the Properties item from the door drop-down menu



- Set the values in the Door Basic tab



- **Name:** Enter Door Name

- Enabled by time zones: enable the settings in the Time zones tab for the Door.

- Type: Select door type. This option will only change the door image/icon in the list underneath the name of the EWS controller, but no changes will be done in system behaviour.

- **Lock release time:** The lock release time can have a value between 1 to 255 seconds. If toggle operation is needed, enter 0.

- **Door has not been closed timer:** The time allowed for the door to be left open after authorized access and before the Door open too long event (alarm) is invoked. If there is no limit, enter 0.

- **Door open too long time:** The time allowed for the door to be open after authorized access and before the Door open too long event (alarm) is invoked. If there is no limit, enter 0.

- Enable door sensor: can be set to enabled or disabled.

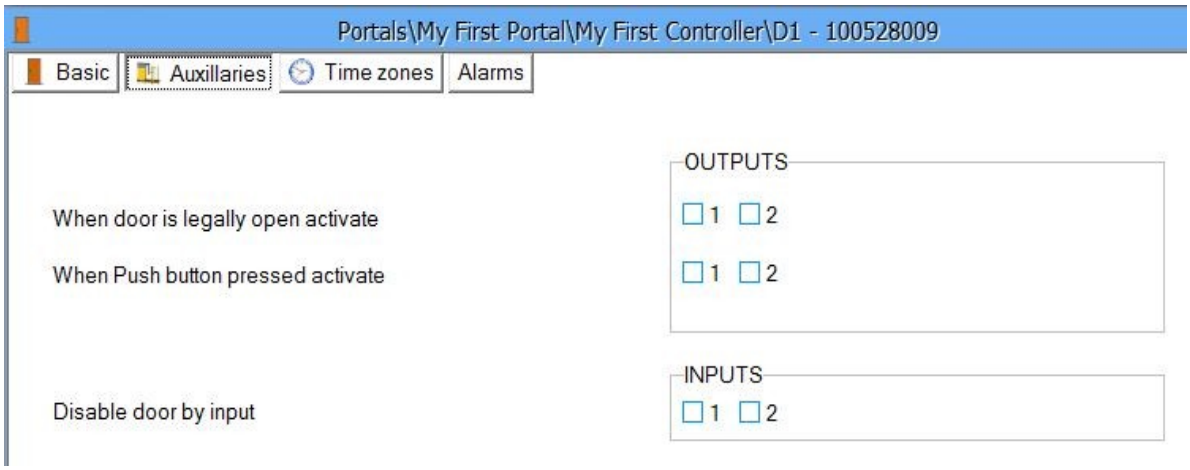
- **Door sensor type:** can be set to Normally Close (NC) or Normally Open (NO), depending on the type of sensor (state at closed door).

- **Push button type:** can be set to Normally Close (NC) or Normally Open (NO).

- **Push button enabled:** allows the door to be opened using the push button.

- Enabled by time zones: enable the settings in the Time zones tab for the Push button.

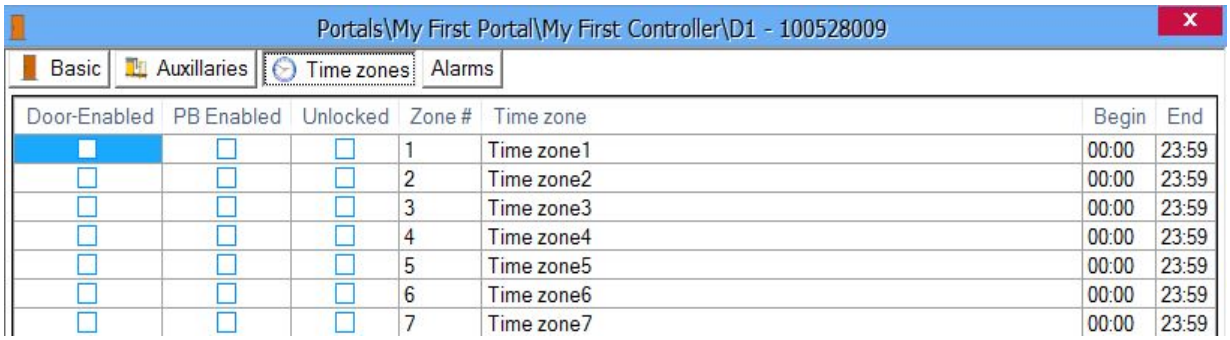
- Set the values in the Auxiliaries tab



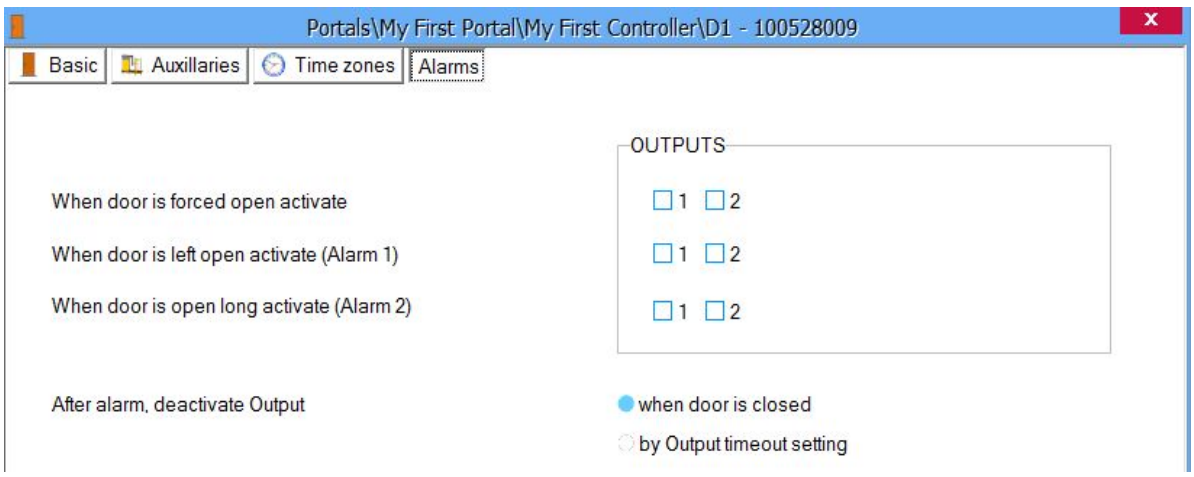
- **OUTPUTS:** Select the door event(s) that will activate the relay outputs (except door relays; door relays follow the authorization rule)

- **INPUTS:** Select if any input should disable the door

- Select the Time zones tab and check the time zones during which the door lock should be released



- Select the Alarms tab



- Assign relays for alarms listed

- After alarm, deactivate Output: the behavior of the output after the alarm has triggered.

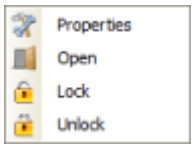
When door is closed: the output will be deactivated when the door is closed.

By Output timeout setting: Output will behave as configured.

- Click on the Save & Exit button
- Repeat the door configuration procedure on the other doors driven by the same controller

Door control

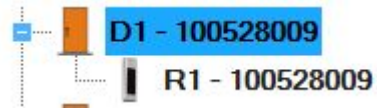
- Right-click on the door to control and select the control item from the door drop-down menu



- **Open:** Acts as legal access to the door, door behavior is the same as normal access
- **Lock:** Locks the door so that it can't be opened by users
- **Unlock:** Cancels the Lock command

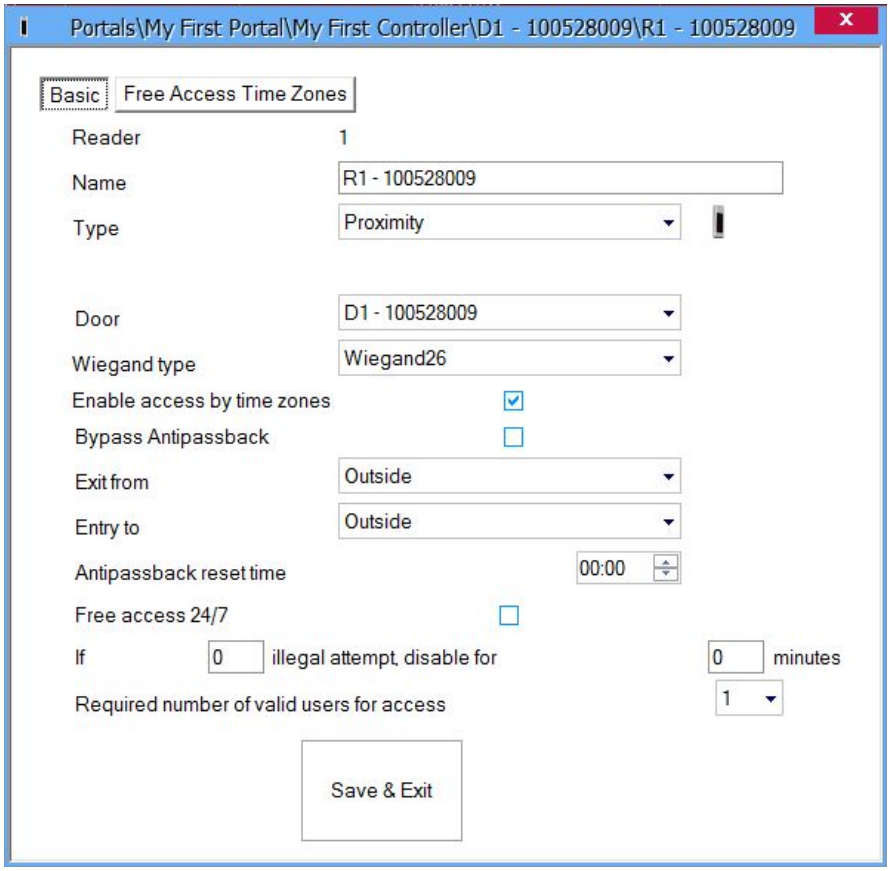
Readers

- Expand the Door item to view the readers

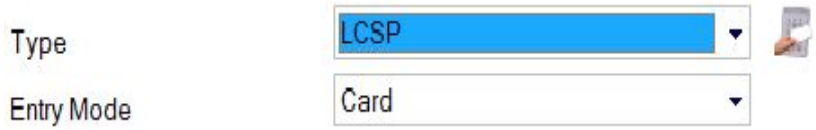


- Right-click on the reader to be configured and select the Properties item from the reader drop-down menu

- Set the values in the Basic tab



- **Name:** Enter the Reader's Name
- **Type:** Select the Reader's Type
- **Entry mode:**This selection is optional and is visible if reader supports different modes of entry. E.g. if using an LCSP card/Access Code reader then four modes of entry are available.



- **Door:** Select which controller door the reader is attached to.
- **Wiegand type:** Select the Wiegand type of the Reader
- **Enable access by time zones:** enables the settings in the Free Access Time Zones tab.
- **Bypass Antipassback:** if this is checked antipassback will not be valid for this reader.
- **Exit from:** set the area which is exited.
- **Entry to:** set the area which is entered.
- **Antipassback reset time:** set the duration time of antipassback.
- **Free access 24/7:** grant all users 24/7 utilisation.
- **In the event of (number) illegal attempts disable for (number) minutes:** set the number of

illegal attempts and the time of disabling the reader.

- **Required number of valid users for access:** Number of different users that must be registered at the reader to grant access.

- Select the Free Access Time Zones.

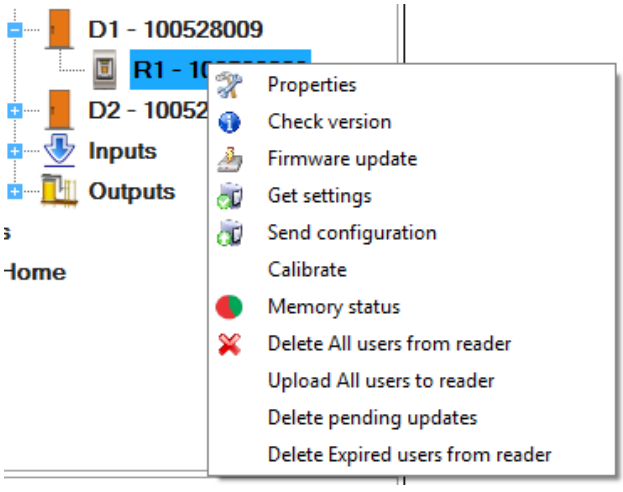
- Apply the time zones for the reader.

- Click on the Save & Exit button

- Repeat the reader configuration procedure on the other readers driven by the same controller

Fingerprint readers

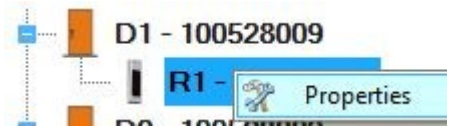
If fingerprint readers are used, additional reader menu items are available



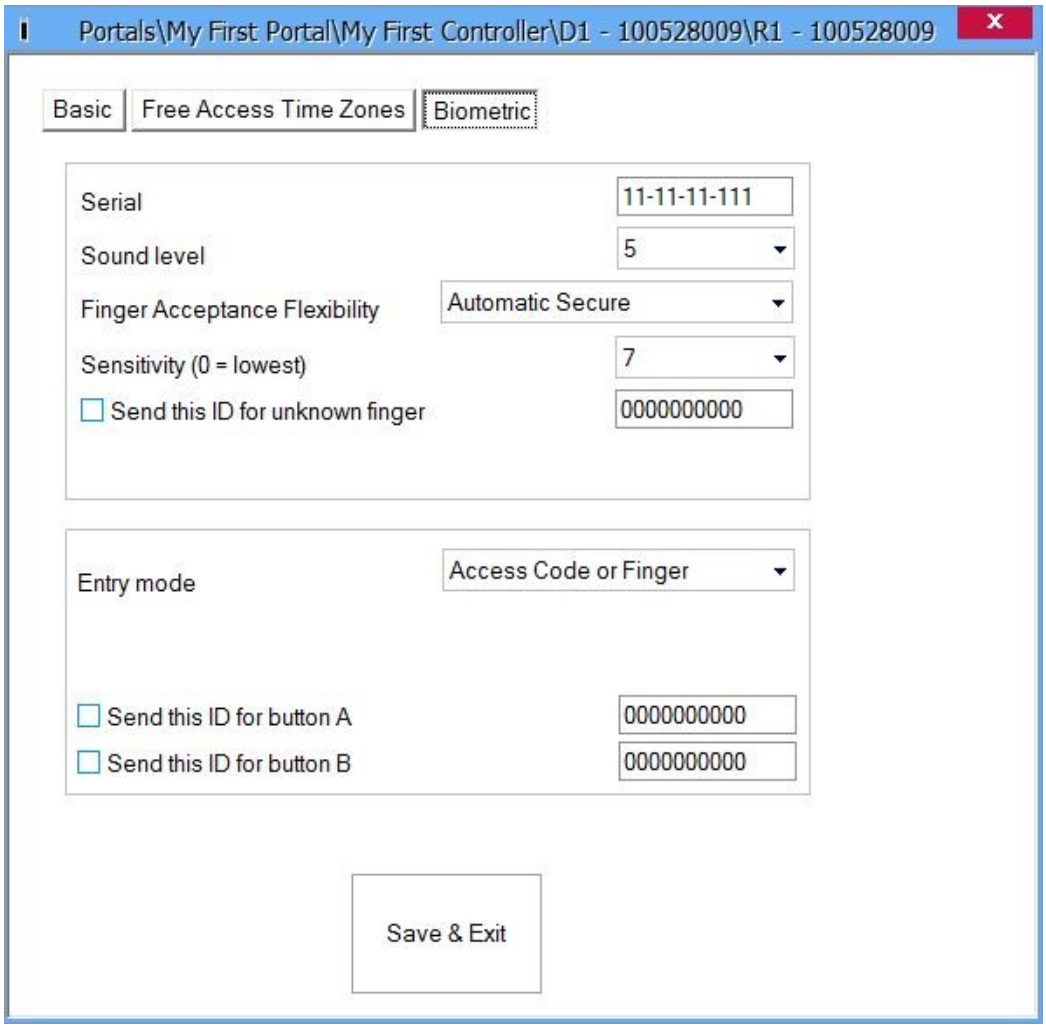
Add or modify a reader

- Expand the Door item to view the readers

- Right-click on the reader to be configured and select the Properties item from the reader drop-down menu



- Set the reader type to one of the fingerprint models in the Basic tab
- Select the Biometric tab and set the values



  - **Serial:** Fingerprint Reader Serial Number
  - **Sound level:** Sound level of the device
  - **Finger Acceptance Flexibility:** Acceptedtolerance. The recommended value is “Automatic Secure”.
  - **Sensitivity:** Bio-sensor sensitivity, the recommended value is 7, most sensitive.
- If devices have a keypad (BioXr, BioXrC), further settings will be available:
  - **Entry mode**:
    “**Finger**” (the keypad is inactive)
    “**Access Code or Finger**” (The Fingerprint Reader will be configured to accept either Access Codes or fingers)

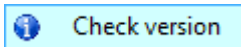
"**Access Code and Finger**" (The Fingerprint Reader will be configured for double security, requiring a Access Code and a corresponding finger. Only the right combination will send the user Wiegand to EWS)

- **Send This ID for:**
  Unknown Finger sends the desired Wiegand when an unknown finger is applied.
  Unknown Access Code sends the desired Wiegand when an unknown Access Code is applied.
  Button "A" Pressed sends the desired Wiegand when button "A" is pressed.
  Button "B" Pressed sends the desired Wiegand when button "B" is pressed.

- Click on the Save & Exit button

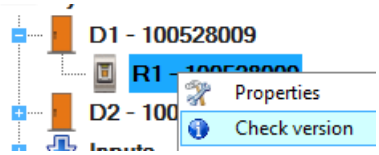
Check firmware version

- Right-click on the reader and select the Check version item

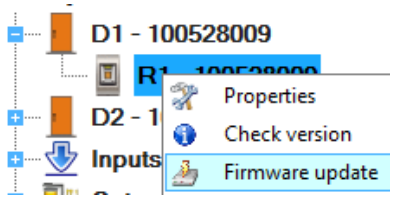


Firmware update

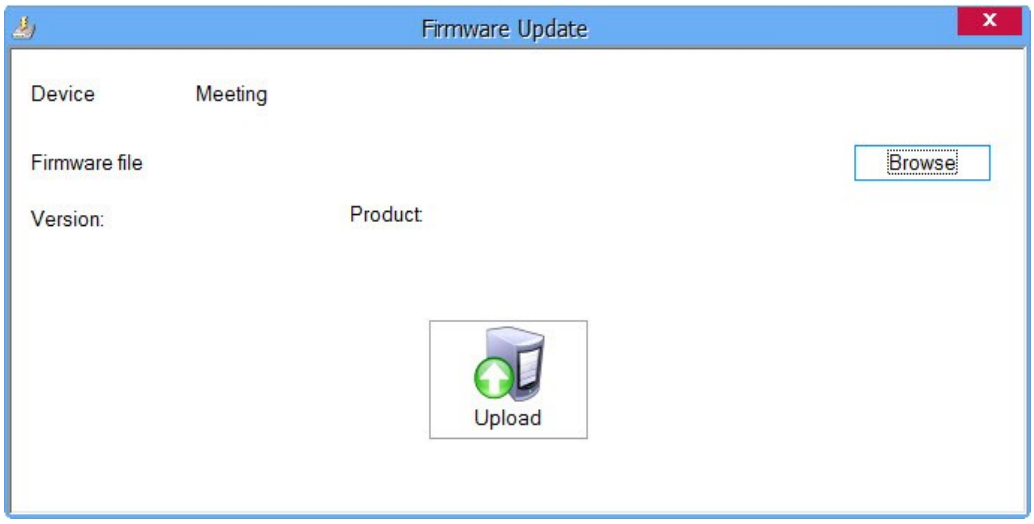
- Check the reader firmware version



- Right-click on the reader and select Firmware update menu



- On the Firmware update window, click on the Browse button. The default location of the firmware files installed with PROS CS Setup is in the Client installation folder under "Firmware" folder. If you have a newer version, use browse to locate it.
- Select the firmware file with a "xhc" extension
- Check the firmware version. If the version is not greater than the existing version of the reader then do not upgrade with this file unless specified by the Installer or manufacturer of the device.
- Click on the Upload button



- After the server starts the update you should receive the following event

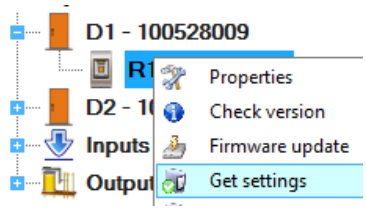
Time	Portal	Controller	Reader	Door	Event
30-Jan-14 10:16:55 AM	My First Portal	My First Controller	R1 - 100528009		Firmware update started

- After the server finishes the update you should receive the following event

Time	Portal	Controller	Reader	Door	Event
30-Jan-14 10:17:51 AM	My First Portal	My First Controller	R1 - 100528009		Firmware update success

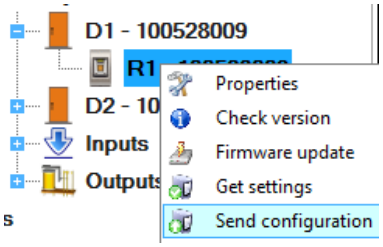
Read reader settings

- Right-click on the reader and select the Get settings menu



Upload configuration to a reader

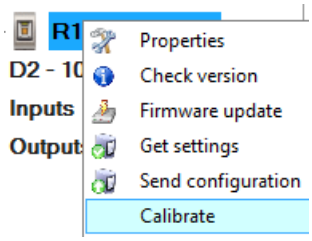
- Right-click on the reader and select the Send configuration menu



- See the events panel to check the configuration flow

Sensor calibration

- Right-click on the reader and select the Calibrate menu



- See the events panel to check the Calibration flow

It is recommended to perform a sensor calibration once the reader has been mounted. Clean the fingerprint sensor before calibration.

Delete All users from reader

Right-click on the Biometry reader then select "Delete All users from reader". This will delete all fingerprints from the biometry reader.

Upload all users to reader

Right-click on the Biometry reader then select "Upload All users to reader". This will add update for the reader per each user which have this reader defined in his Access Level or have Access Level = "Unlimited".

Delete pending updates

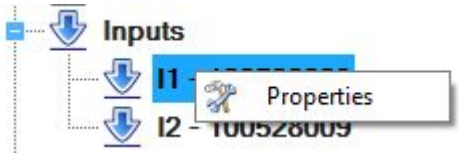
Right-click on the Biometry reader and then select "Delete pending updates". This will delete ALL pending updates for this Reader.

Delete Expired users from reader

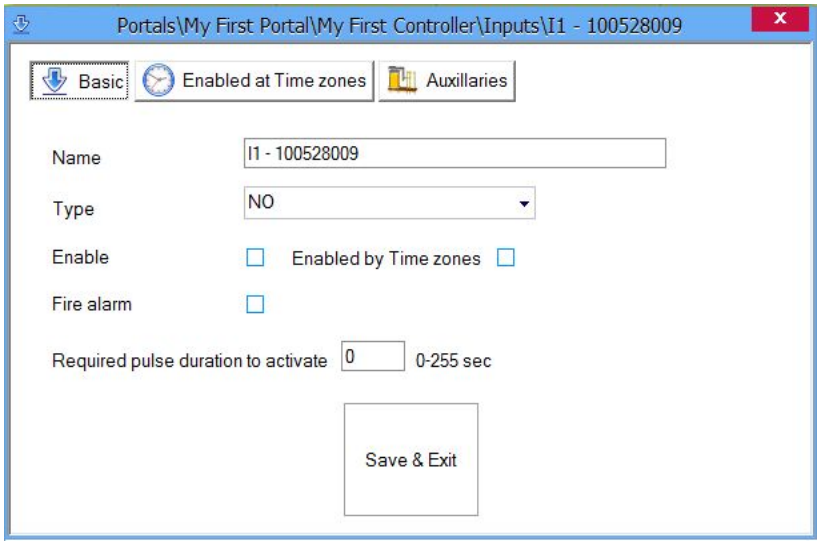
Right-click on the Biometry reader and then select "Delete Expired users from reader". This will delete all expired users in the software from this Reader. (Expired user = user who's "Valid To" parameter is less than today)

Inputs

- Right-click on the input to configure and select the Properties item from the input drop-down menu

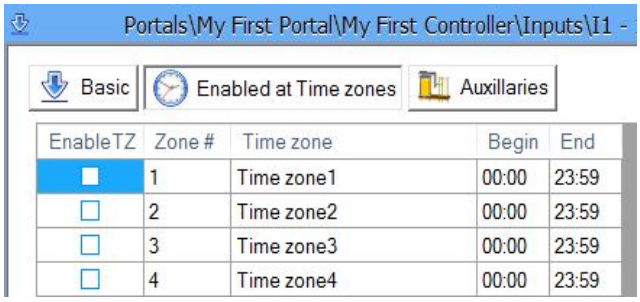


- Set the values in the Basic tab

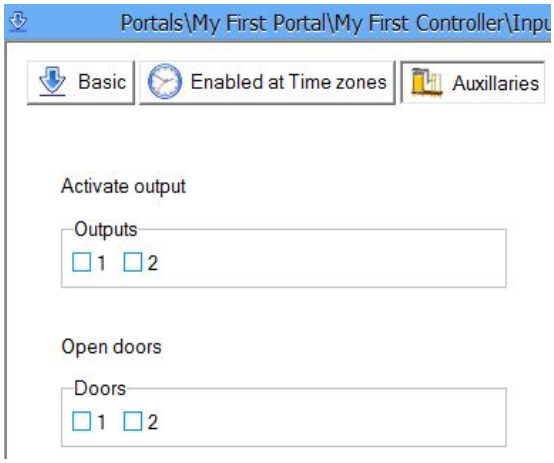


- **Name:** Type Input Name
- **Type:** Select the normal state of the contact energizing the input (NO = no voltage on input, NC = input powered)
- **Enable:** Check to enable input
- **Enabled by Time zones:** Check if you need to enable time periods
- **Fire alarm:** Dedicate input to Fire alarm input
- **Required pulse duration to activate:** Set the length of time of the signal required to trigger the input.

- If Enabled (Time zones are checked), set the time zones for which the input is enabled



- Set the Auxiliaries options

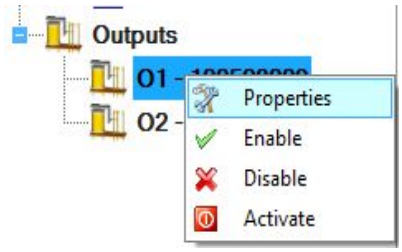


- **Activate outputs:** Outputs to be triggered on input activation
- **Open doors:** Doors to be released on input activation

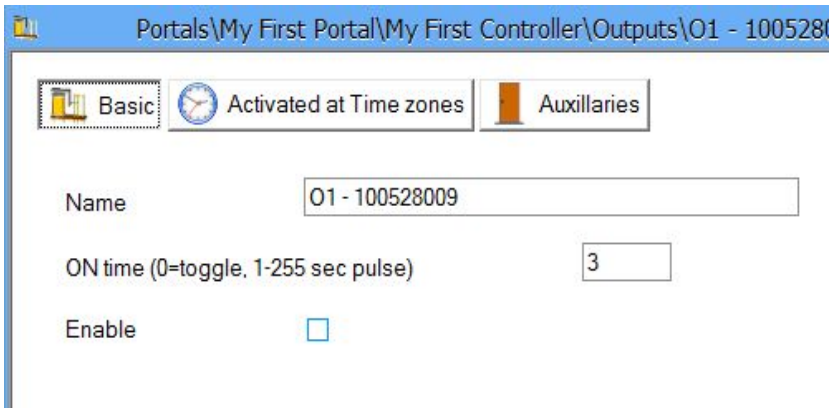
- Click on the Save & Exit button
- Repeat the reader configuration procedure for the other inputs available on the same controller

Outputs

- Right-click on the output to be configured and select the Properties item from the output drop-down menu



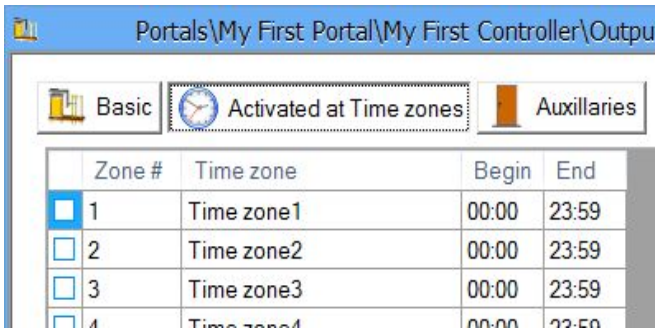
- Set the values in the Basic tab



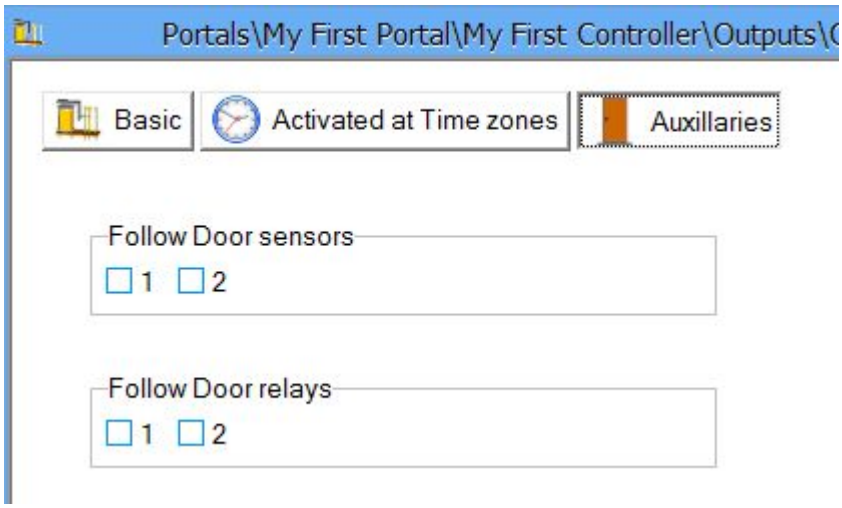
- **Name:** Type the Output Name
- **ON time:** Select how long the output relay should stay energized. Enter 0 to toggle the relay state on event.

- **Enable:** Check to enable output

- Select the Activated at Time zones tab if you need to use the output as a time activated relay



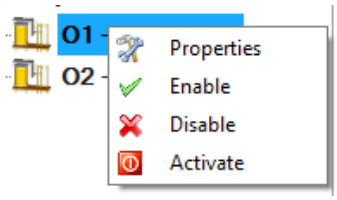
- Click on the Auxiliaries tab to select if the output relay should follow the door sensors or door relays



- Click on the Save & Exit button
- Repeat the output configuration procedure on the other outputs available on the same controller

Output control

Right-click on the output to be controlled and select the control item from the drop-down menu

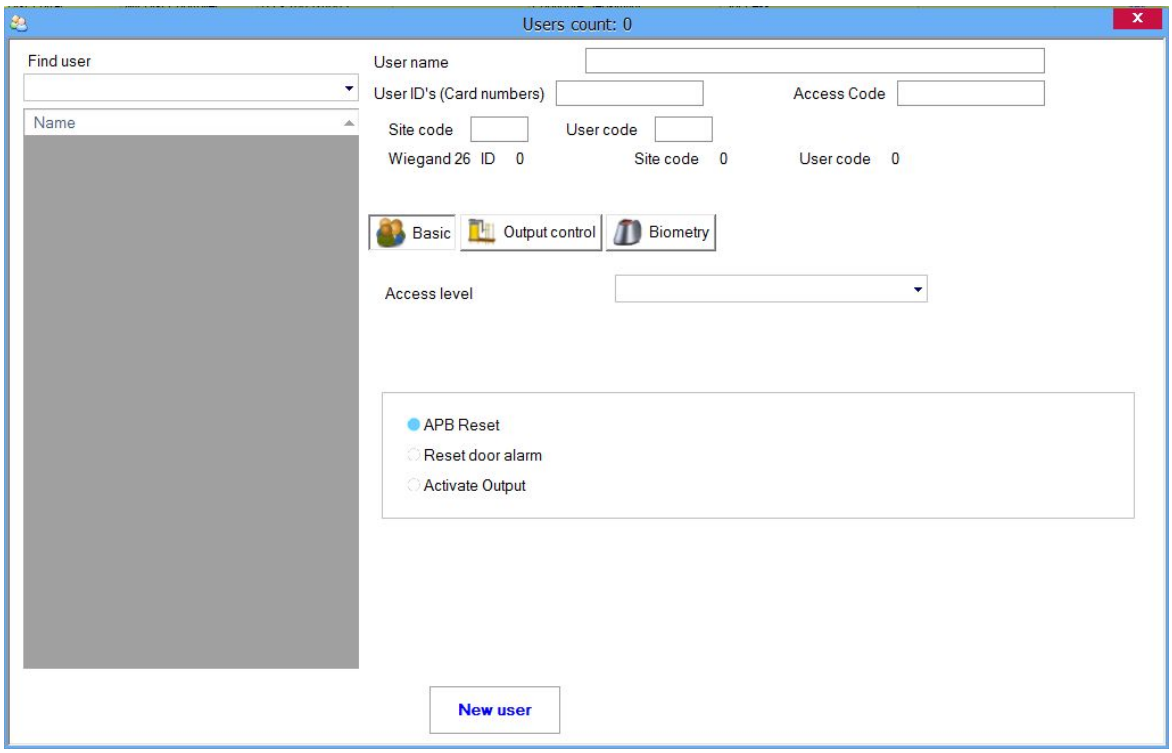


- **Enable:** Enables output
- **Disable:** Disables output
- **Activate:** Output responds as programmed to behave when it is ON

Function cards

Function cards are special type of users that can invoke some action from the access controller. These cards cannot be used for access.

Double-click on the Function cards icon in the Users Panel.



Function cards can be managed in a same way as users.

Function cards will be valid on EWS controllers having readers in selected Access levels.

The action of the function cards will be conducted only on EWS controllers where the card is presented.

A function card can be used as an access Access Code or Finger print.

Functions:

APB reset: Controller will reset APB status of all users to "nowhere".

Reset door alarm: If the door alarm is activated, presenting the function card will reset the alarm. If the door is not closed, the alarm will be triggered ON again after periods defined in the door alarm settings.

Activate Output: Presenting the function card will activate the selected outputs in the "Output control" tab.

Sites

Site can be defined as grouping of the controllers by their geographical location. It is used to keep track of users current location and for generating the evacuation report.
Example:

1. If a company has 2 buildings, then it will have 2 sites - "Building 1" and "Building 2".
2. If a company has offices in 3 cities in the country,then it will have 3 sites - "City 1", "City 2", "City 3"

By default there is only one site defined in the software, named "Home". It can be renamed but not deleted.

Adding new site:

- Right click on the "Sites" icon in the hardware section
- Click on "Add site"
- Enter the name of the new site in the text box
- Click on "Add & Exit"
- The new site will appear in the sites section

Modifying existing site:

- Right click on the site you want to edit
- Click on "Properties"
- Enter the new name of the site
- Click on "Save & Exit"

Deleting site:

- Right click on the site you want to delete
- Click on "Delete"

After creating all sites, all controllers need to be assigned to their appropriate site. This can be done in controller properties in the "Properties" tab.

Areas

Each site contains multiple areas. For example if the site represents 1 building, then it will have 2 areas - Inside and Outside area. Another example is to mark each floor in the building to be a separate area. So if the building has 5 floors then the site will have 5 areas.
These areas "Inside" and "Outside" are defined by default in the site "Home" and cannot be deleted.

Adding new area:

- Right click on the site you want to add areas
- Click on "Add area"
- Enter the name of the new area in the text box
- Click on "Add & Exit"
- The new area will appear bellow the site icon

Modifying existing area:

- Right click on the area you want to edit
- Click on "Properties"
- Enter the new name of the area
- Click on "Save & Exit"

Deleting area:

- Right click on the area you want to delete
- Click on "Delete"

After creating all areas, all readers belonging to these areas need to be configured according to their area. This can be done in reader properties, in the "Basic" tab. Set the parameters "Exit from" and "Entry to" according to the area this reader belongs. For example if there is a site (building) with outside reader for access control, and this site has two areas - "Inside" area and "Outside" area, then you will set "Exit from" =

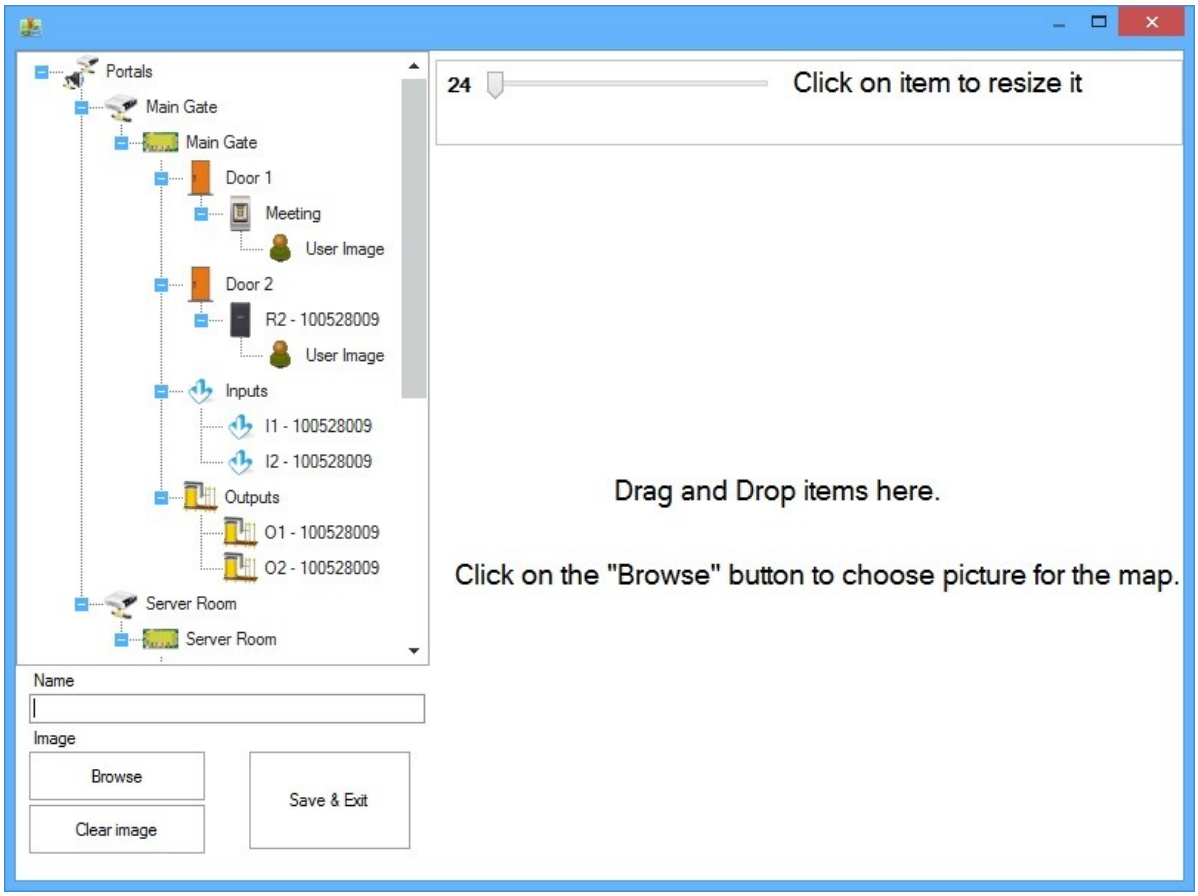
"Outside" and "Entry to" = "Inside".

Maps

Maps are used to have visual display on your hardware installation. They contain a map picture and hardware items.

Creating a map

- Right click on the Maps icon in the hardware section
- Click on "Add map"
- New window for setting up the map will appear



- Enter the name of the map in the "Name" text box
- Click on the "Browse" button to choose the background picture for the map
- Drag and drop items from the left to the map. Items that can be dragged are: Door, Reader, User Image, Input, Output.
- Resize the item from the toolbox on the top
- Move the item by dragging it on the map
- Choose whether you like the item properties (Name, Last Event) to be shown on the map
  checked = Show on map
  unchecked = Hide on map

- When selecting an item in the item list on the left, if it exists on the map it will be selected
- When selecting an item on the map, it will be selected in the item list on the left
- No duplicate items are allowed on the map

- Click on "Save & Exit" to save the map
- The new map will appear bellow the "Maps" icon in the hardware section

Modifying a map
- Right click on the map that needs to be modified
- Click on "Properties"
- Modify the map
- Click on "Save & Exit"

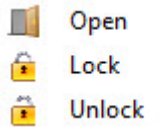
Delete a map
- Right click on the map
- Click on "Delete"

Using the maps

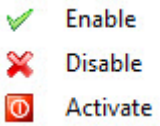
Right click on the map icon and then click on "Show map". The map window will appear onscreen

Each event from the Events window in the software is shown in the map, if the corresponding item for that event exists on the map.

If the item supports user control then it is available in the right click menu of the item.
- Right click on the "Door" item to display the following menu



- Right click on the "Output" item to display the following menu



Note:

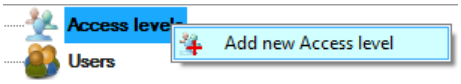
- Several map windows can be open at the same time.
- If the map windows are left open while closing the software, next time the software is started, each map window will be shown at the same location as it was before.

Access settings

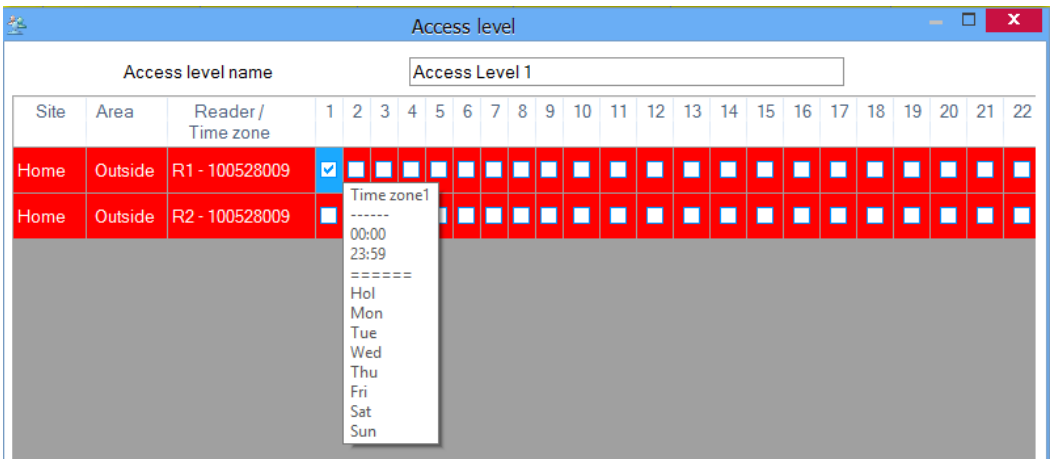
Access levels

Adding Access level

- Right-click on the Access level main item in the Users Panel and click on "Add new Access level"



- Enter the Access level name



- Check the Allowed access time zones for each reader. Each column represents one time zone. Setting access depends on the row color.

  - **Green color:** Reader is set for access without a time zone schedule. Access on this reader will be

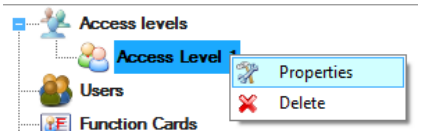
granted if any time zone field for this reader is checked. Access will be denied if none of the fields are checked.

- **Red color:** Reader is set to grant access by time zones. Access will be granted if the event is within any of the checked time zones. Time zone settings for each reader/Time zone can be checked by holding the mouse cursor over the checkbox as shown above.

- Click on the Save & Exit button

Edit access level

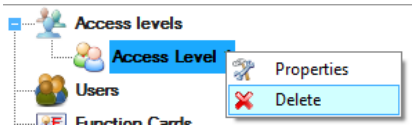
- Expand the access level item in the Users Panel, right-click on the Access level and select the "Properties" menu item



- Edit the Access level
- Click on the Save & Exit button

Delete Access Level

- Expand the Access Level item in the Users Panel, right-click on the Access level and select the "Delete" menu item. The Access Level cannot be deleted if any users are assigned to it.

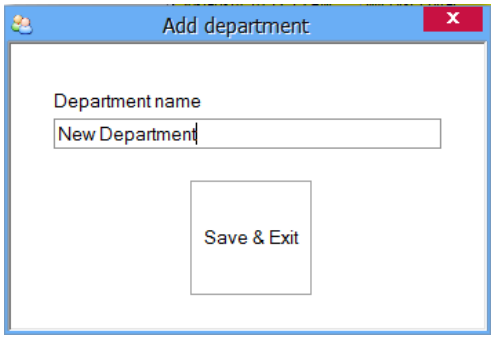


Departments

Add a Department

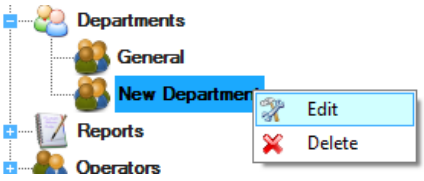
- Right-click on the Departments item in the Users Panel and click on "Add new"

- Enter the Department name and click on the save & Exit button

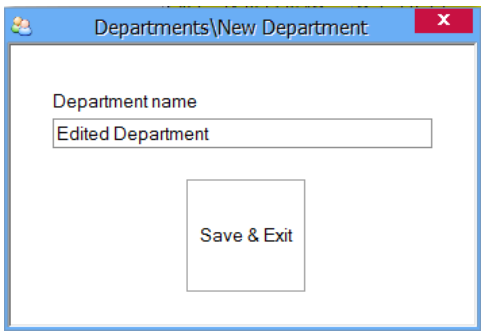


Edit a Department

- Expand the Department item in the Users Panel, right-click on the Department and select the "Edit" menu item



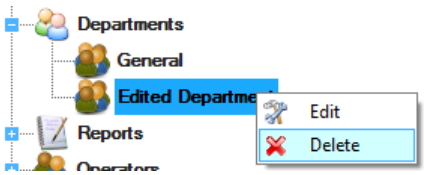
- Edit the Department name



- Click on the Save & Exit button

Delete a Department

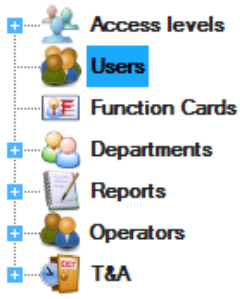
- Expand the Department item in the Users Panel, right-click on the department and select the "Delete" menu item.



- Default department "General" can not be deleted.

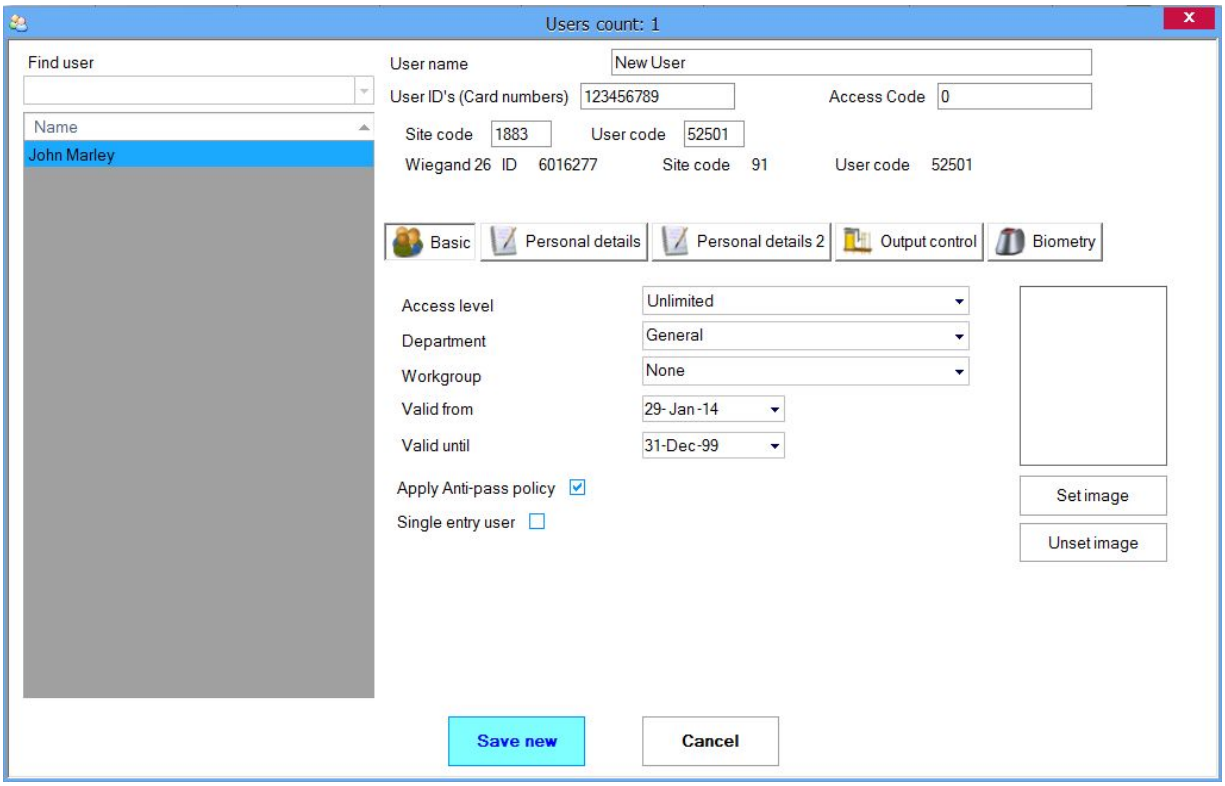
Users

Double-click on the Users item in the Users Panel to open the Users window



Add a user

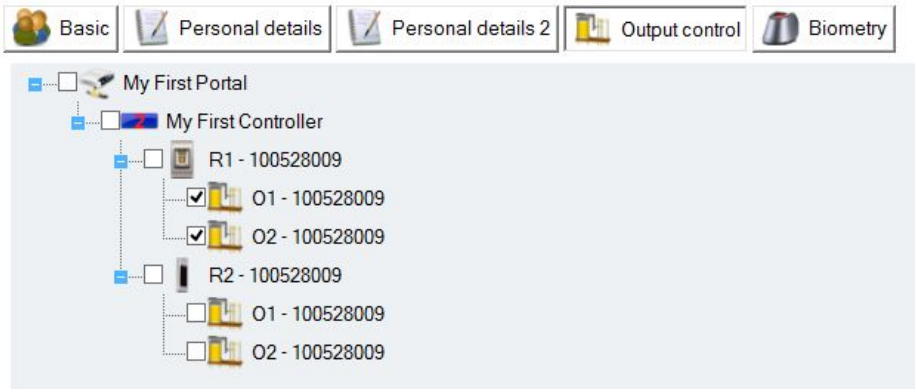
- Click on the New User button



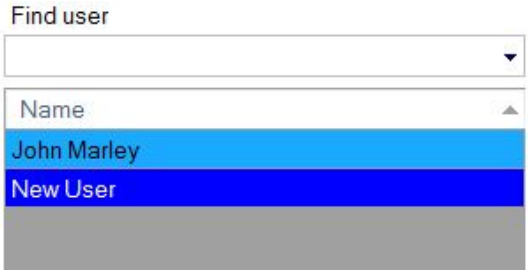
- Enter the Name of the User
- Enter theUser ID (card number). If there are two numbers on the card with values less than 65536 then use the Site code and the User code box.
- Enter Access Code if in the system will be used devices with keypads
- Select the Access level from the Access level drop-down list box
- Select the Department from the drop-down list box
- Select Workgroup
- Select the from-until validity period
- Click on the Set image button and then browse for the User's image
- If **Apply Anti-pass policy** option is checked, user must behave by APB settings of the readers, otherwise user will have no APB restriction.
- **Single entry user:**A User will have one-time entry an all readers defined by user access level. If the user has used his/her one-time entry, on the next upload of the user in the EWS controller, one-time entry will be renewed.

- Fill Personal details of the user if required in the Personal details tabs.

- If the User should activate some outputs (not door relays), click on the Output control tab to select outputs



- Click on **Save**
- The entered User is added to the user table on the left side



Edit a user

- Select the User to be modified in the users table on the left side of the Users window

- Click on the Edit button
- Modify the user data (including the name if required)
- Click on the Save button

Delete a user

Warning!

Deleting a user erases the user from database. If you need to keep an activity record of the user, you can change the access level to "No access" instead of deleting the user, or generate the necessary reports and save them to a file (PDF is recommended), before deleting the user.

- Select the user to be deleted in the users table on the left side of the Users window

- Click on the Delete button

Fingerprints

Read me first

Selecting a finger for fingerprint enrollment

At least two fingerprints should be enrolled for each user in case of any abnormal situation like having an injured finger or carrying an object by hand.
In case of low recognition, the user can register the same fingerprint twice to increase the recognition rate.
It is recommended to use the index or middle finger. If you choose another finger, the recognition rate may be decreased because it tends to be more difficult to place the finger in the center of the sensor area.

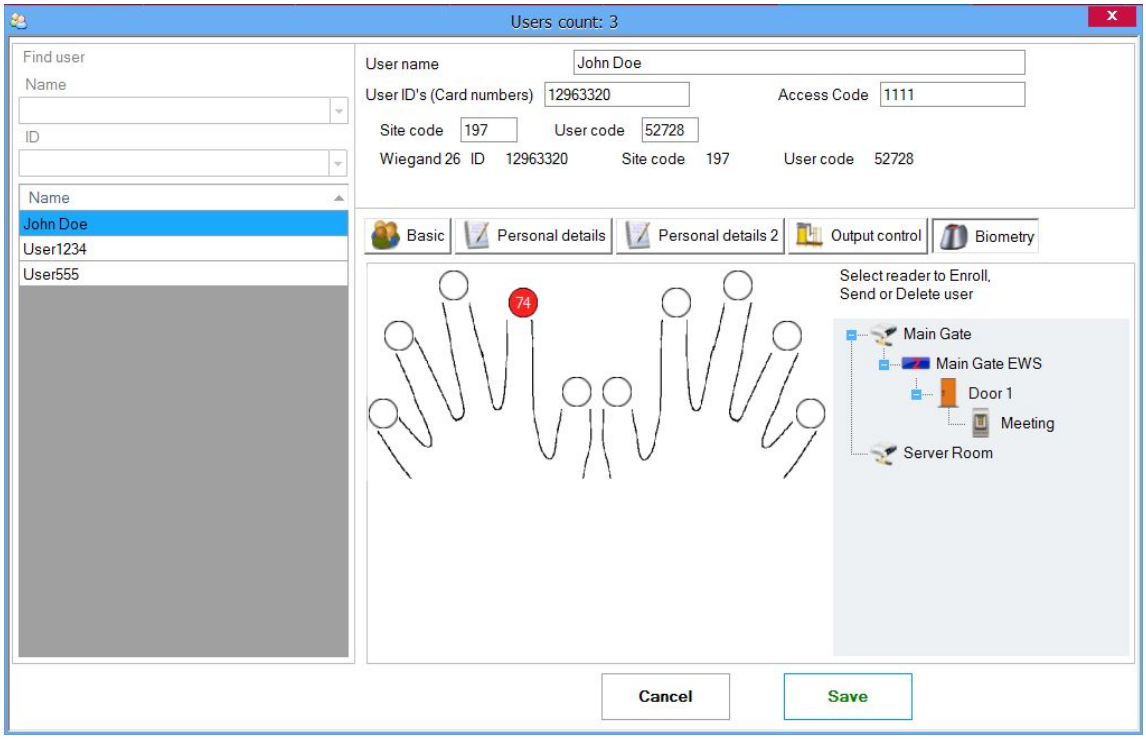
Caution while registering a fingerprint

The initial fingerprint registration is important.
Because the recognition process compares the scanned fingerprint with the registered one, an abnormally registered fingerprint can cause a failure.

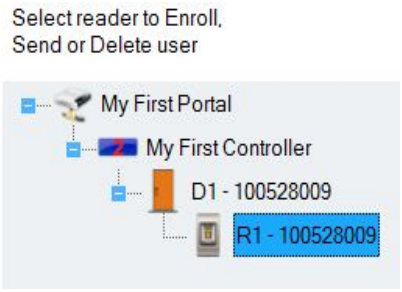
1. Put the center of your fingerprint on the middle of the sensor
2. If you have a cut on your finger or your fingerprint is not clear enough, retry with another finger
3. When the fingerprint recognition is in progress, do not move your fingerprint

Enrolling Fingerprints from a reader

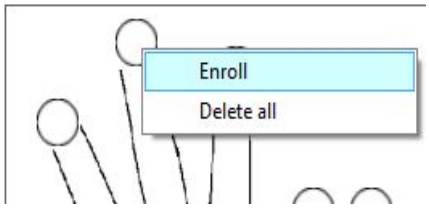
- Select the User in the User Column, click on the Edit button and then select the Biometry tab.



- Select the Fingerprint reader from where the enrollment will be done.



- Right click on the fingertip and select “Enroll”.



- Present the finger on the selected reader and the finger tip will turn red, with the percentage of successful enrollment shown next to the fingertip.

- Repeat the procedure for the other fingers (as required)

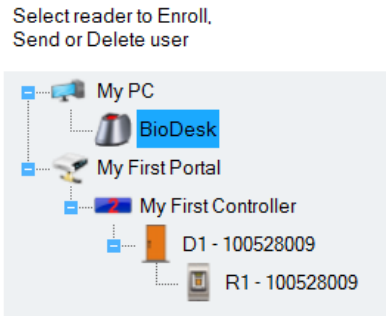
Note: If more fingerprints are added for one user, all fingers will send the same Wiegand Code to the controller.

Enrollment from a desktop Reader

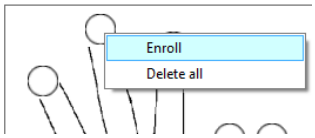
Install the Desktop Reader (BioE) using the drivers located on the CD provided with the Fingerprint Reader. It is installed in the same way as a USB Device. When the desktop reader has been installed it will automatically appear in the Software.

- Select the User in the User Column, click on the Edit button and then select the Biometry tab.

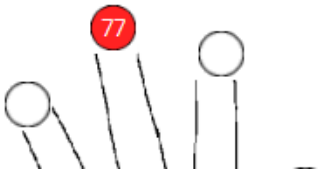
- Select the desktop reader from where the enrollment will be done.



- Right click on the fingertip and select “Enroll”.



- Present the finger on the selected reader and the finger tip will turn red, with the percentage of successful enrollment shown next to the fingertip.



- Repeat the procedure for the other fingers (if needed)

Note: If more fingerprints are added for one user, all fingers will send the same Wiegand Code to the controller.

Uploading the fingerprints to the Fingerprint readers

Right-click on each Biometry reader and then select "Upload All users to reader". This will add update for the

reader per each user which have this reader defined in his Access Level or have Access Level = "Unlimited".

Deleting Fingerprints

In General, after enrolling fingers and saving the user, the fingerprints are stored in the Fingerprint Reader and in the Software.

Deleting can be done only in the software, only in the readers or from both places.

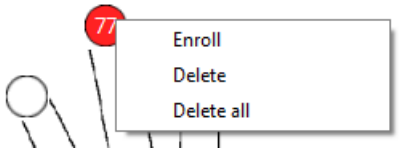
Deleting all users from the fingerprint Reader

- Right-click on the Biometry reader then select "Delete All users from reader". This will delete all fingerprints from the biometry reader.

Deleting user finger templates from the Software

- Select the User.

- Go to the fingertip that needs to be deleted, right click and select ”Delete” for one finger or “Delete All” for all fingers of the User. With this procedure the User’s fingerprints are deleted from the software and updates are added for deleting them from the reader too.



Upload all fingerprints to reader

Right-click on the Biometry reader then select "Upload All users to reader". This will add update for the reader per each user which have this reader defined in his Access Level or have Access Level = "Unlimited".

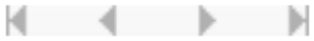
Reports

To generate reports expand the Reports item in the User panel.

All reports are shown on the report window with following buttons:

- Export - save report to disk or send it to mail recipient in various file formats (PDF, Excel, Text…)

- Print - print report

 - Navigation - to view the First page, Previous page, Next page, Last page

- Find - search for specific text in the report

User list report

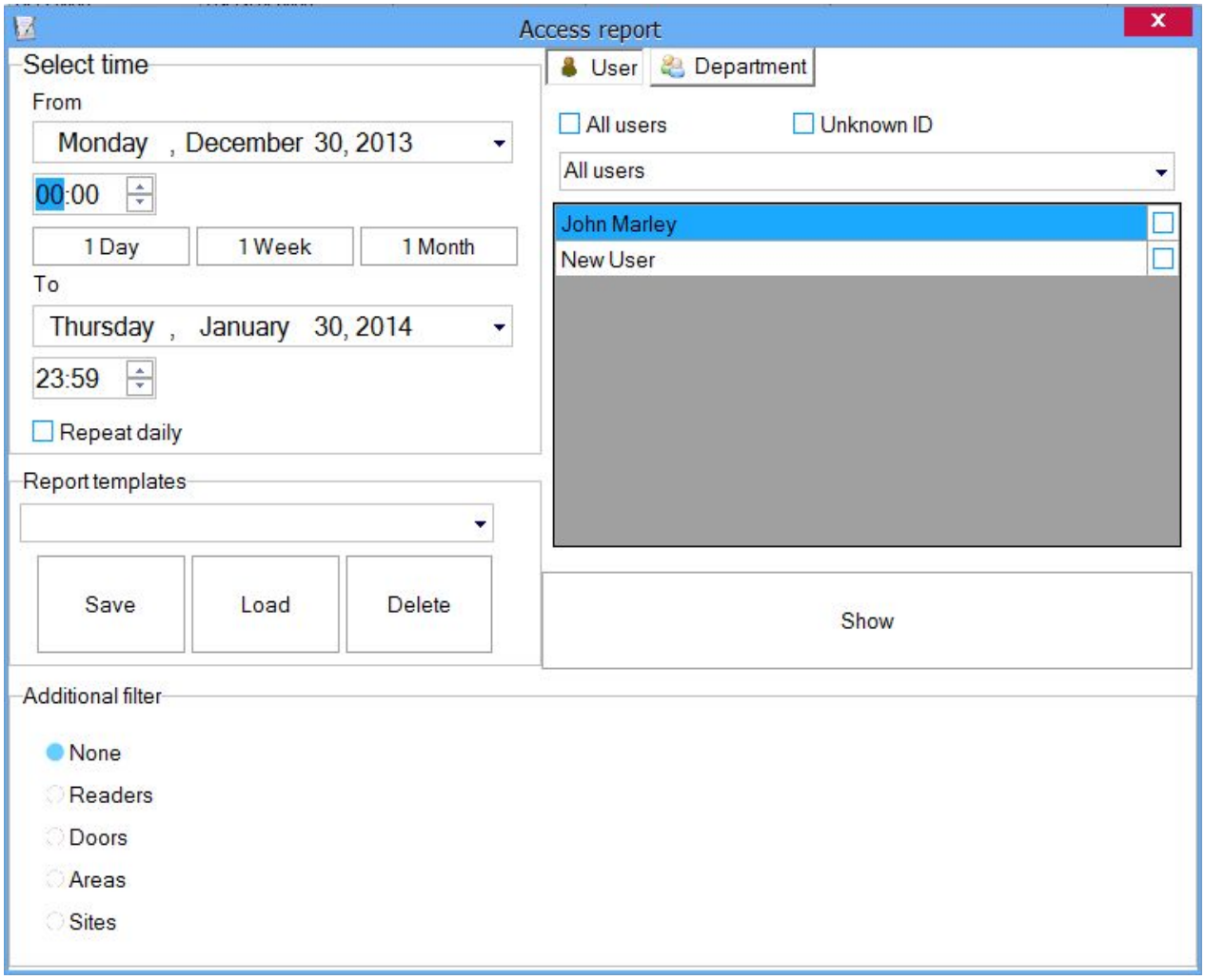
- Double-click on the ID item in the expanded Reports item
- Wait for the report to be generated as shown

User		ID	Access level	Workgroup
Guest 1		20763	Unlimited	
Guest 2		165243	Unlimited	
Jey Low		14678	Unlimited	
John Do		23831	Unlimited	
Mary Ex	dtyud	13720704	Unlimited	
Michael Smit		24820	Unlimited	Sytech
Stiven Senal		25004	Unlimited	
Temp 1		15584	Unlimited	
Temp 2		13271	Unlimited	

Access reports

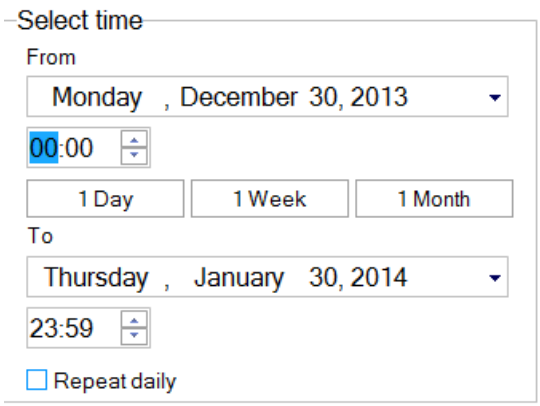
Load report window

- Double-click on the Access item in the expanded Reports item to open the Access report window



Set time filters

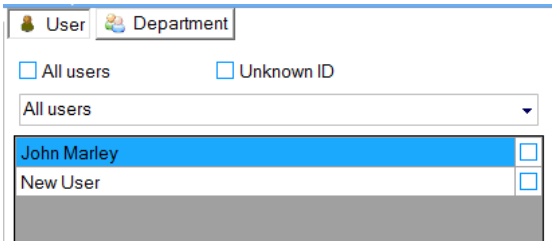
- Select time period



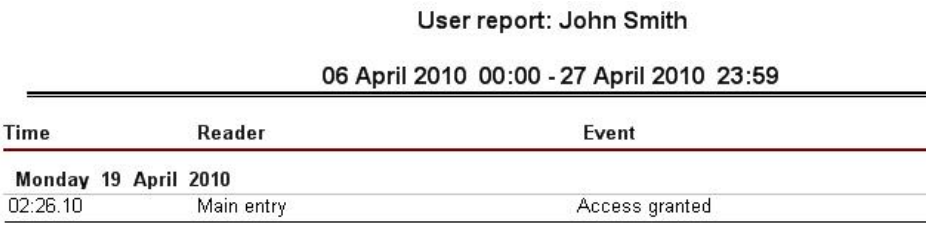
  - If Repeat daily is checked, reports will be generated for the selected time range of the day, every day in the selected days range
  - There are 3 shortcut buttons for setting period of 1 Day, 1 Week or 1 Month. You just need to set the Date From and click on some of the buttons

User report

- Set time filters
- Select the User tab in the Basic filter panel

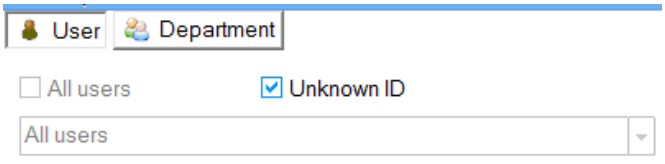


- Select the user name from the drop-down list box
- For more than one user report select users by checking them at check boxes at right side
- For a report of all users, check the "All users" item
- Click on the Show button at the bottom of the Basic filter panel to load the report



Unknown ID report

- Set time filters
- Select the User tab in the Basic filter panel
- Check "Unknown ID"



- Click on the Show button at the bottom of Basic filter panel to load the report

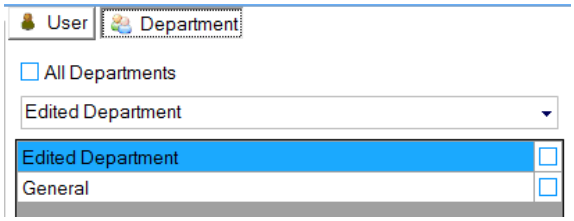
Unknown ID Report

01 June 2010 00:00 - 05 June 2010 23:59

Time	ID	Reader	Event
Tuesday 01 June 2010			
21:59.18	456456	Main Entry	Access denied = ID unknown
22:06.03	456456	Main Entry	Access denied = ID unknown
22:52.15	456456	Main Entry	Access denied = ID unknown

Department report

- Set time filters
- Select the Department tab in the Basic filter panel



- Select the department from the drop-down list box
- For more than one department report select users by checking them at check boxes at right side
- Click on the Show button at the bottom of Basic filter panel to load the report

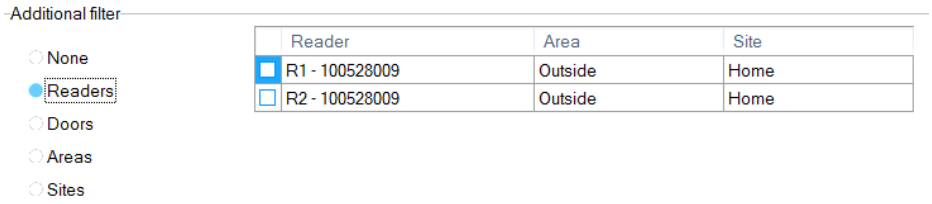
Department report: General

06 April 2010 00:00 - 20 April 2010 23:59

Time	User	Event	Reader
Monday 19 April 2010			
02:26.10	John Smith	Access granted	Main entry

Adding a reader filter to Access report

- Set time filters
- Set filter for User or Department report
- Select the Readers in the additional filter panel



- Click on the Show button at the bottom of Additional filter panel to load the report

All users report

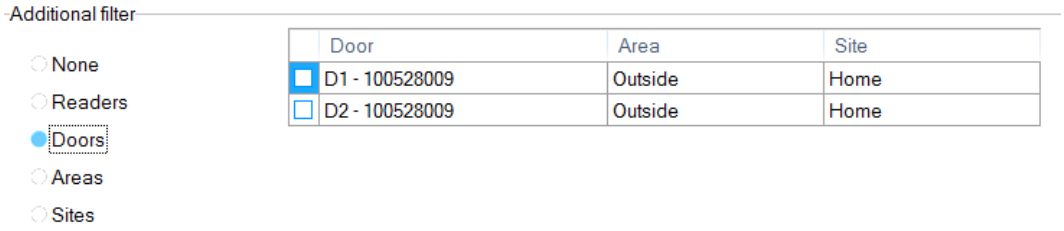
06 April 2010 00:00 - 20 April 2010 23:59

At readers: Main entry

Time	User	Reader	Event
Monday 19 April 2010			
02:26.10	John Smith	Main entry	Access granted

Adding a Doors filter to Access report

- Set time filters
- Set the filter for User or Department report
- Select the Doors in the additional filter panel



- Click on the Show button at the bottom of the Additional filter panel to load the report

User report: John Smith

06 April 2010 00:00 - 20 April 2010 23:59

At doors: Main door

Time	Reader	Event
Monday 19 April 2010		
02:26.10	Main entry	Access granted

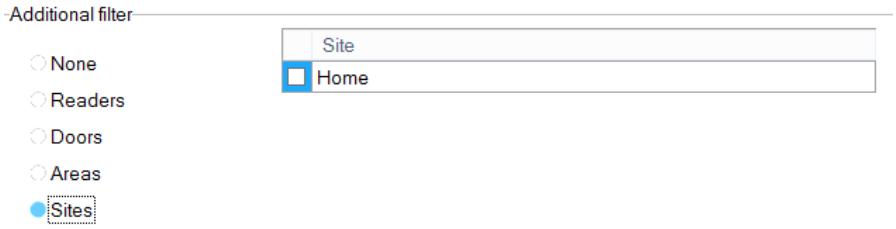
Adding an Areas filter to Access report

- Set time filters.
- Set the filter for User or Department report.
- Select the Areas in the additional filter panel.

- Click on the Show button at the bottom of the Additional filter panel to load the report.

Adding a Site filter to Access report

- Set time filters.
- Set the filter for User or Department report.
- Select the Sites in the additional filter panel.



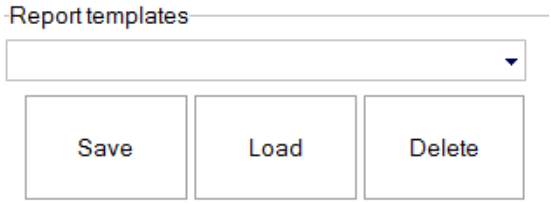
- Click on the Show button at the bottom of the Additional filter panel to load the report.

Saved report template

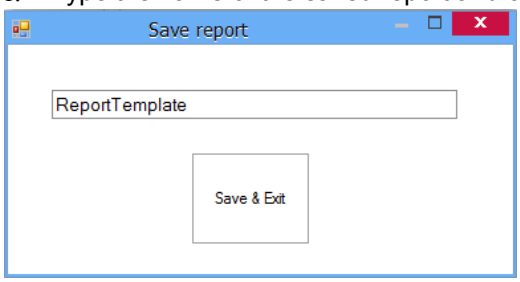
Parameters selected for a report can be saved for future use. All settings and values in the report window will be saved except date values.

Save report template

- Set desired settings in the report window
- Click on Save button

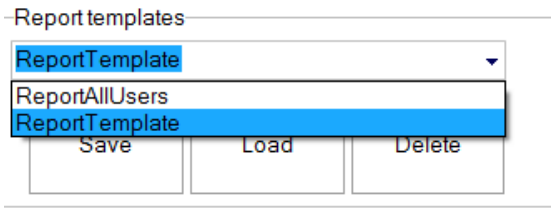


1. Type the name of the saved report and click the Save & Exit button.



Generate report from template

- Select the template and click on the Load button.



1. Set the desired date period and click on the Show button.

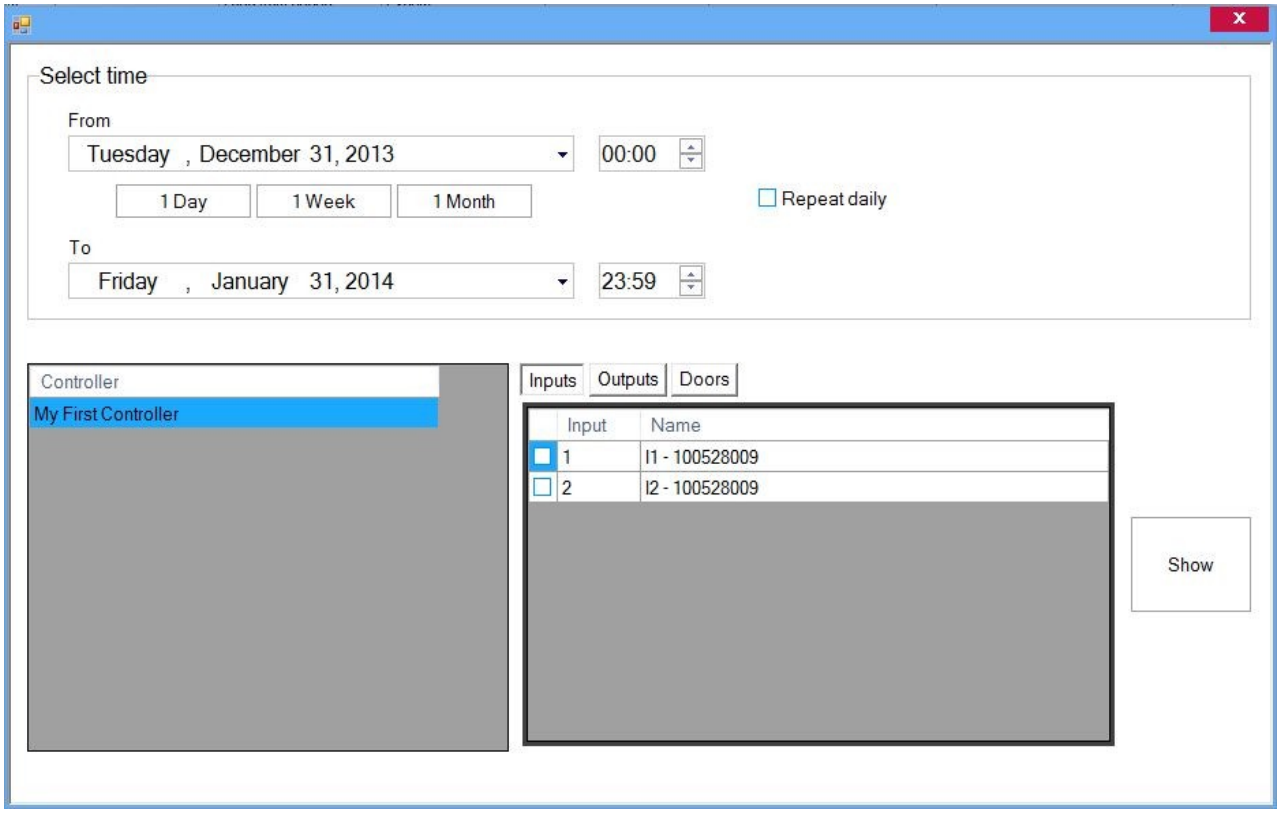
Delete saved template

1. Select template to delete and click on Delete button.

I/O reports

Load report window

- Double-click on the Access item in the expanded Reports item to open the IO report window



Set time and controllers filters

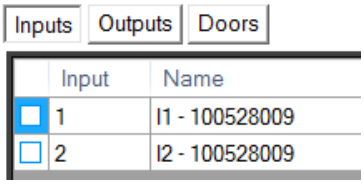
- Select days and time period

- If Repeat daily is checked, reports will be generated for the selected time range of the day, every day in the selected days range
- There are 3 shortcut buttons for setting period of 1 Day, 1 Week or 1 Month. You just need to set the Date From and click on some of the buttons

- Select controller in the Controller table

Inputs report

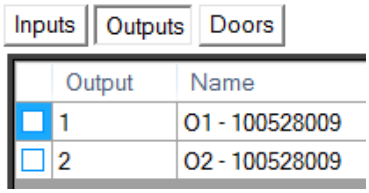
- Set time and controller filters
- Select the Inputs in the additional filter panel



- Click on the Show button load report

Outputs report

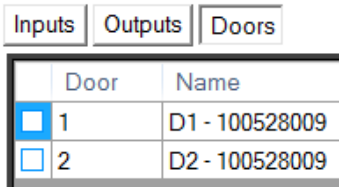
- Set time and controller filters
- Select the outputs in the additional filter panel



- Click on the Show button load report

Doors report

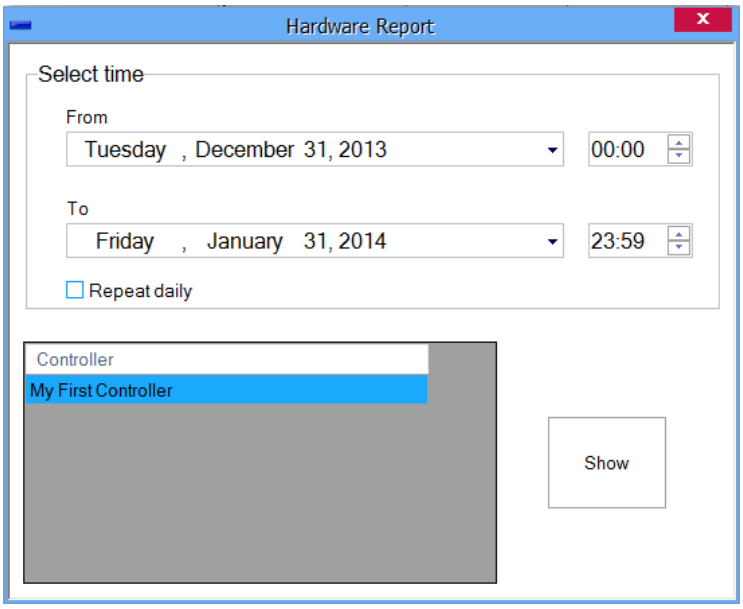
- Set time and controller filters
- Select the Doors in the additional filter panel



- Click on the Show button load report

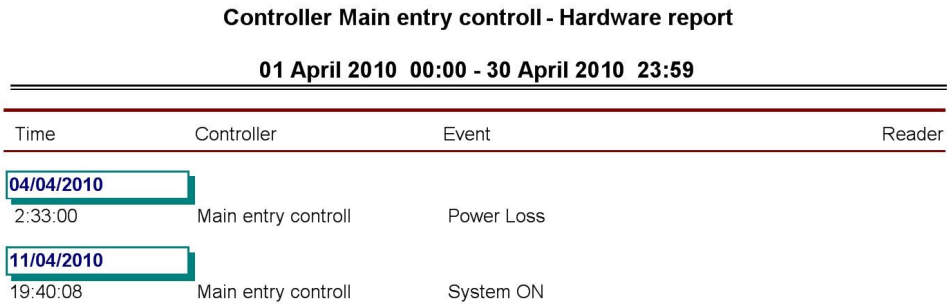
HardwareReport

- Double-click on the Access item in the expanded Reports item to open the Hardware report window



- Select days and time period
    - If Repeat daily is checked, reports will be generated for the selected time range of the day, every day in the selected days range
- Select controller in the Controller table

- Click on the Show button load report



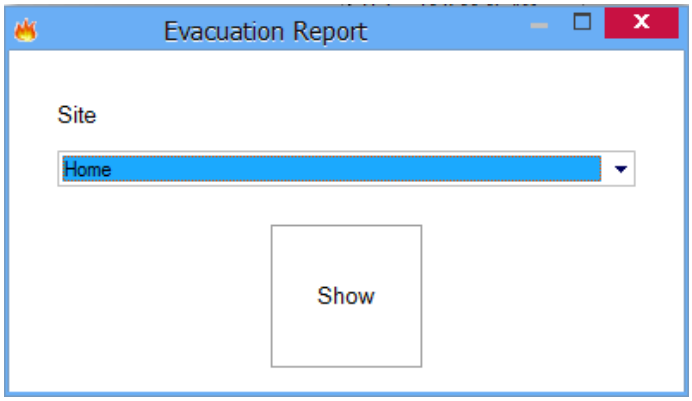
Controller Main entry controll - Hardware report

01 April 2010 00:00 - 30 April 2010 23:59

Time	Controller	Event	Reader
04/04/2010			
2:33:00	Main entry controll	Power Loss	
11/04/2010			
19:40:08	Main entry controll	System ON	

Evacuation report

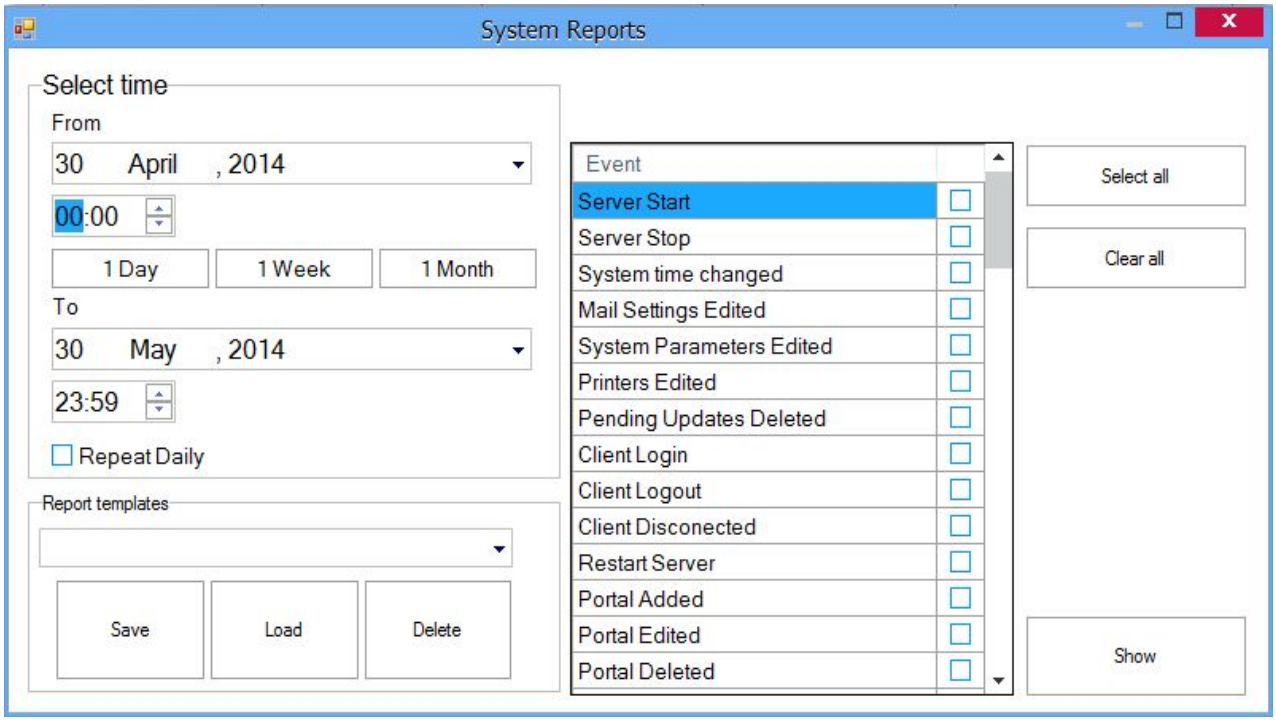
- Double-click on the Evacuation report item to open **Evacuation Report** window



- Select a site and click the Show button
    - The report will show a list of users according to the last event in the site. All users that have any kind of access event within the selected site will be listed by the last event.
    - If for example an evacuation report is to be made on a certain site but a user's last activity is reported from a different site, the user will not be listed in the evacuation report.

System reports

- Double-click on the System report item to open **System Report** window



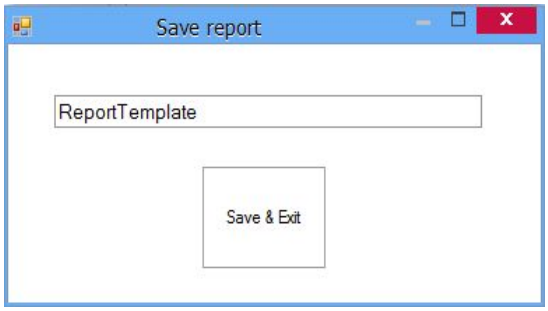
- Select days and time period
    - If Repeat daily is checked, reports will be generated for the selected time range of the day, every day in the selected days range
- Select Events from the event list by checking the boxes in the list
- Click on the Show button

Parameters selected for a report can be saved for future use. All settings and values in the report window will be saved except date values.

Save report template

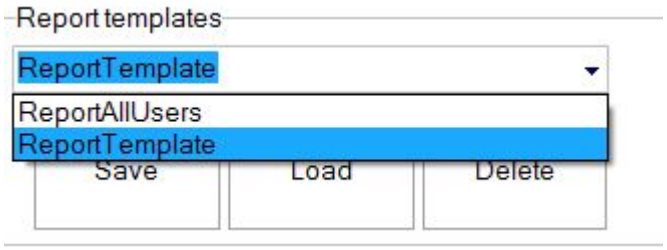
- Set desired settings in the report window
- Click on Save button

1. Type the name of the saved report and click the Save & Exit button.



Generate report from template

- Select the template and click on the Load button.



1. Set the desired date period and click on the Show button.

Delete saved template

1. Select template to delete and click on Delete button.

Program operators

Program options	Operator options					
	Hardware configuration	User management	Operator management	Report view	Program	Access system online

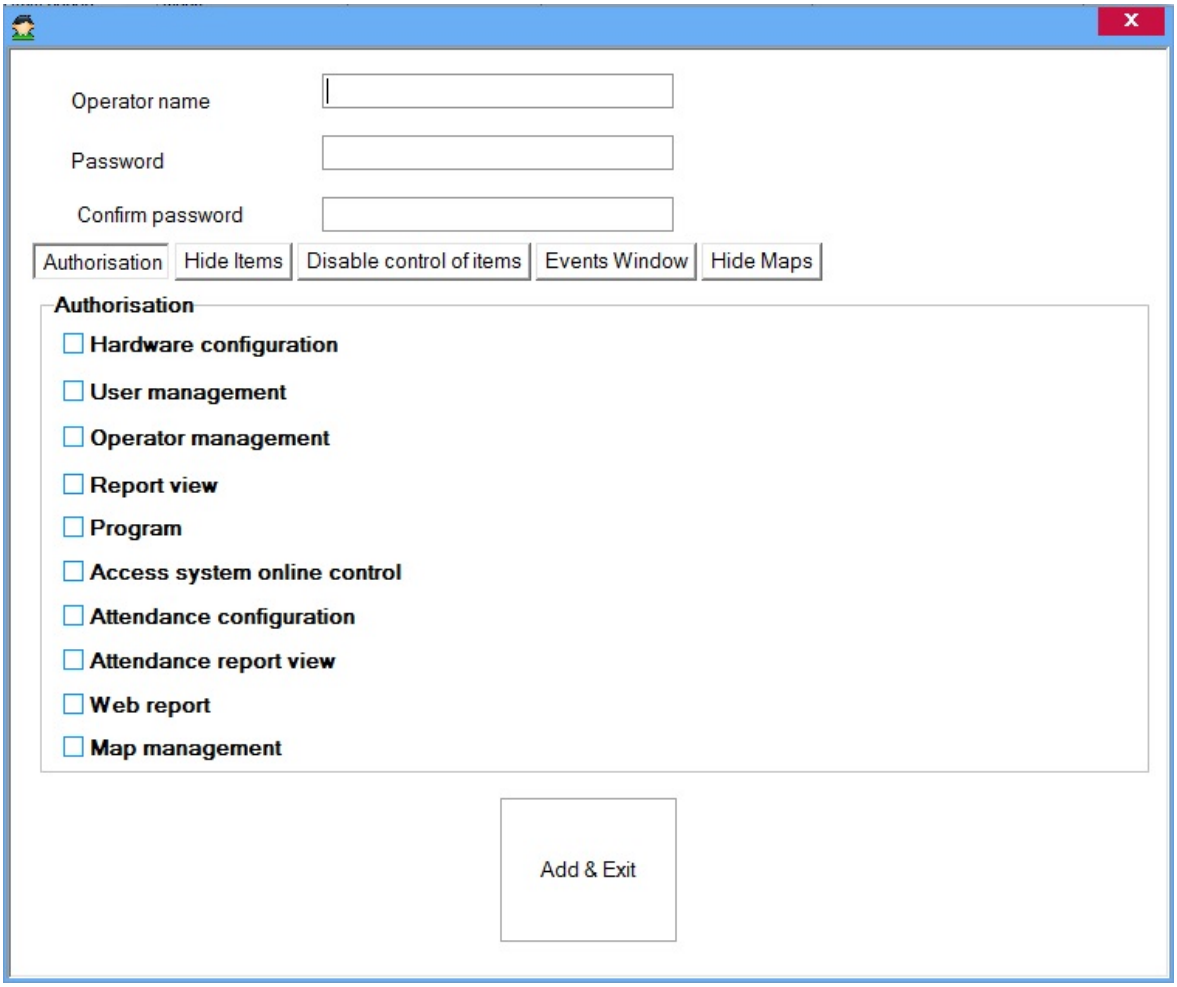
						contro
Main menu						
System parameters					-	
Panels view settings					-	
Upload table		-				
Portals menu						
Add portal	-					
Search portals	-					
Portal menu						
All options	-					
Controller menu						
Modify properties	-					
Start pulling					-	-
Stop pulling					-	-
Configure controller	-					
Set controller time	-					-
Reload keys		-				
Delete controller	-					
Firmware update	-					
Check version online	-					-
Read settings from controller	-					-
Reader menu						
Modify properties	-					
Enable reader	-					
Disable reader	-					
Check version online	-	-			-	-
Firmware update	-					
Read settings from reader	-	-				-
Configure reader	-					
Calibrate sensor	-	-				-
Input menu						

Modify properties	-					
Door menu						
Modify properties	-					
Open door	-					-
Lock door	-					-
Unlock door	-					-
Output menu						
Modify properties	-					
Enable	-					-
Disable	-					-
Activate	-					-
Operators						
All options			-			
Access levels						
All options		-				
Departments						
All options		-				
User management						
All options		-				
Reports						
All options				-		

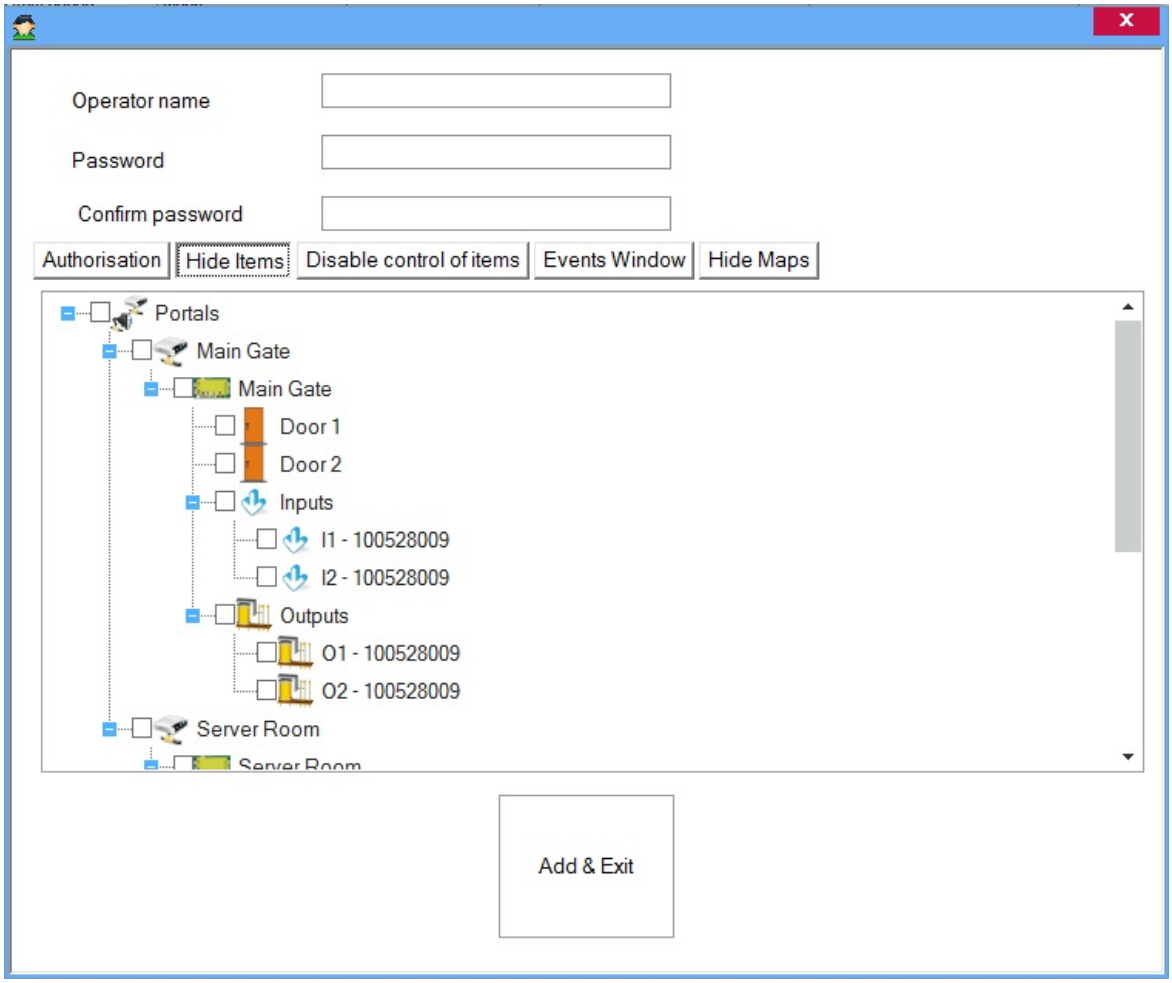
Add an operator

- Right-click on the Operators menu in the User panel and select Add operator

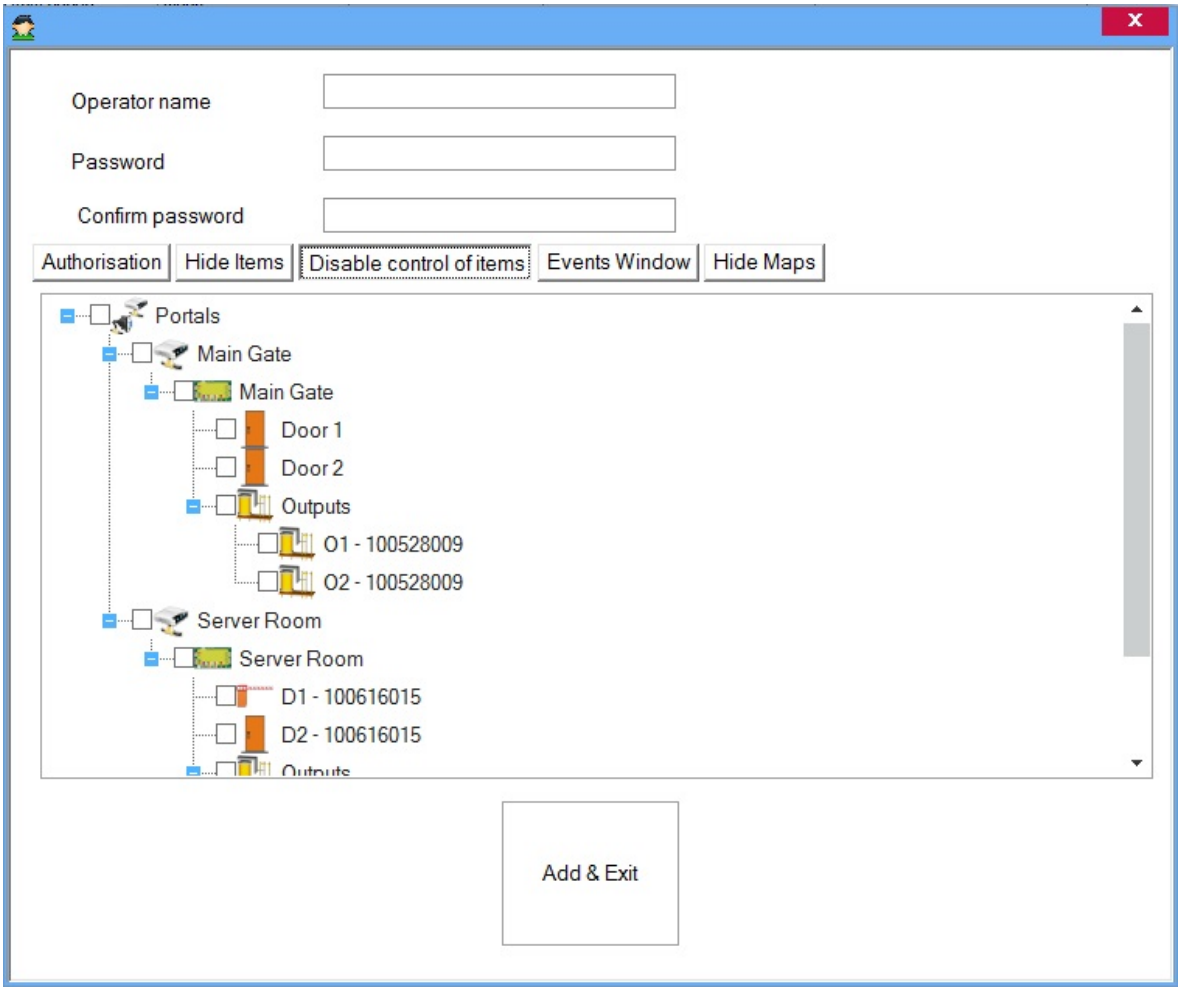
- In the Operator window enter the Name, Password and select the operator's options



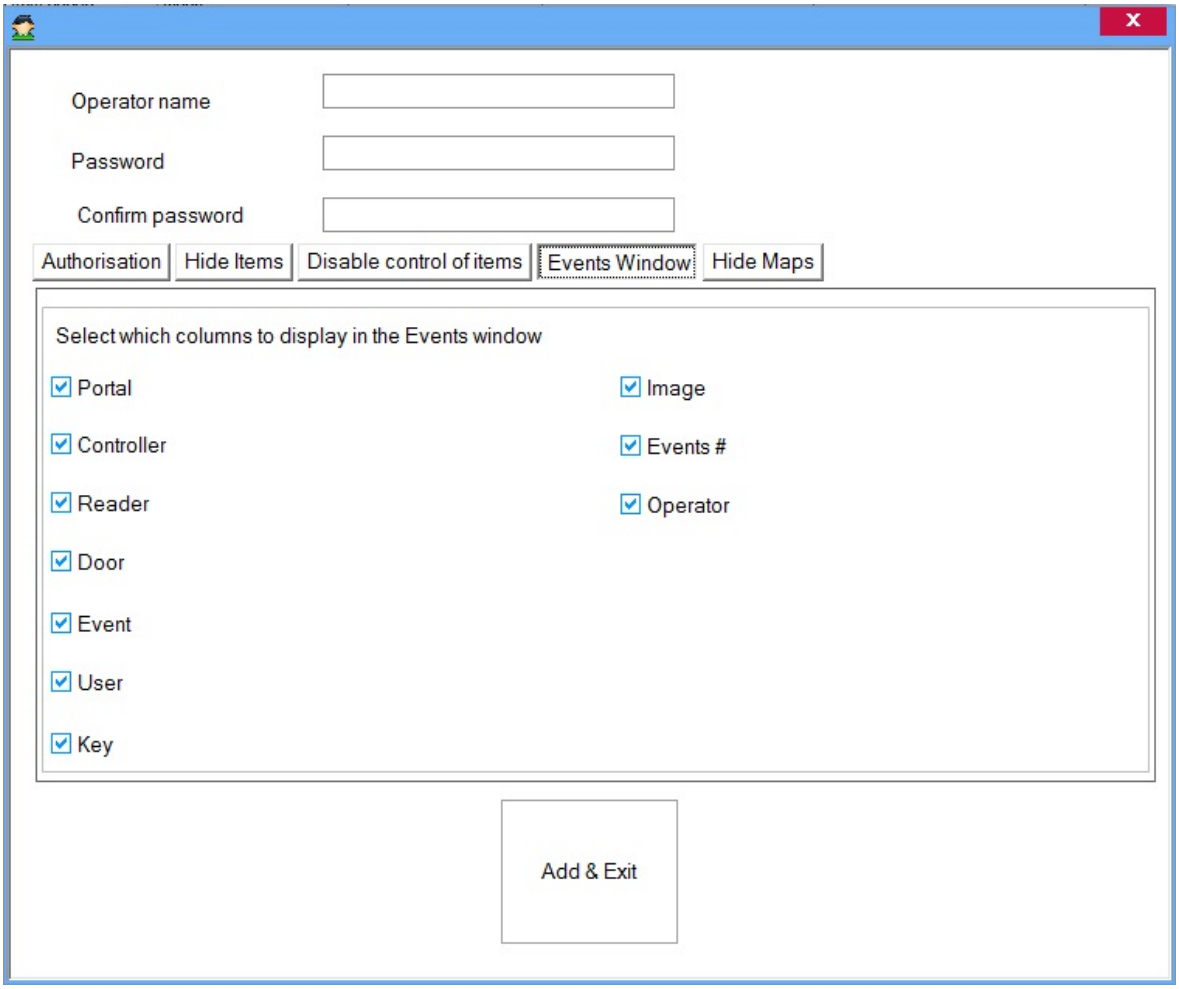
- In the "Hide Items" tab you can choose which hardware items and events from this items will not be shown when logging with this operator.



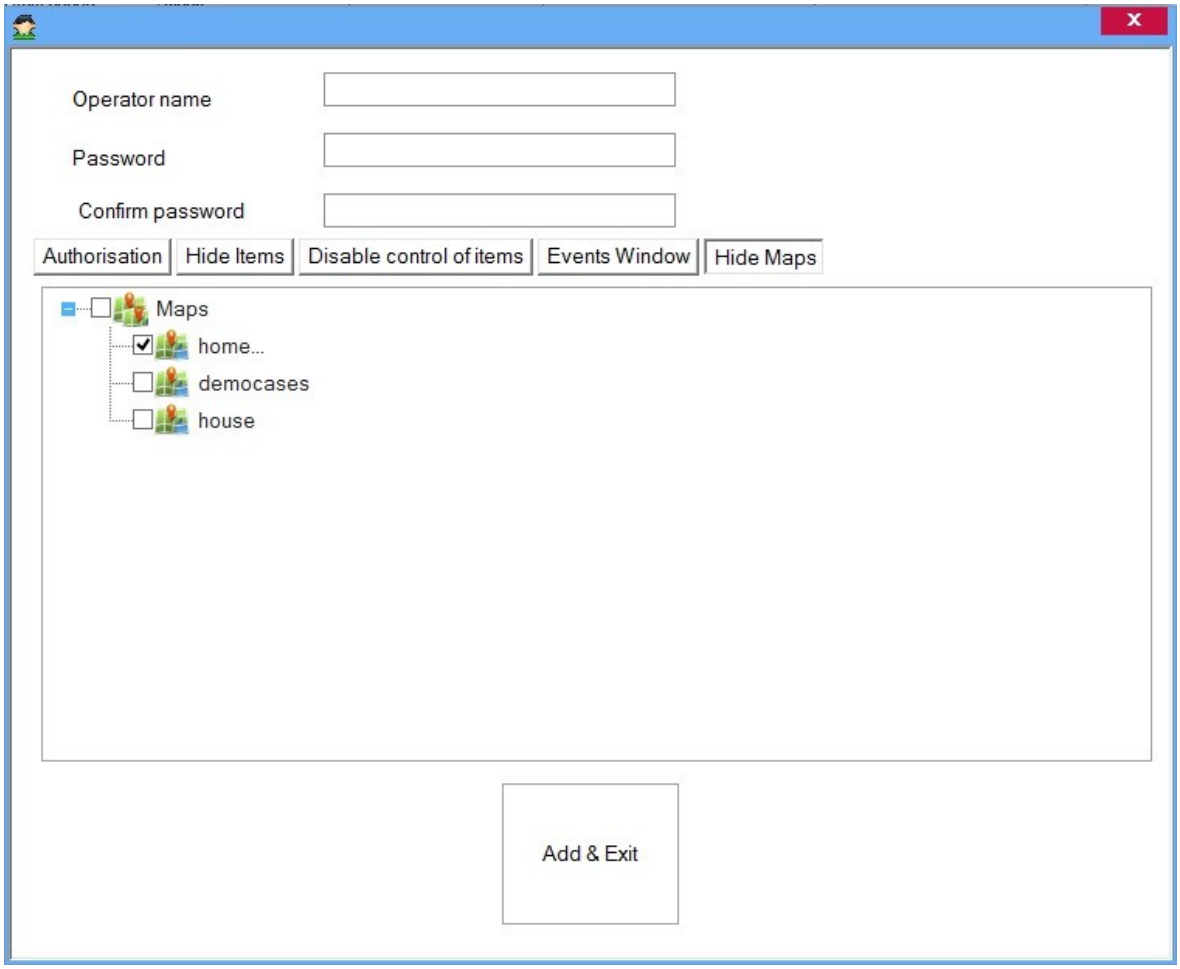
- In the "Disable control of Items" tab you can disable control of hardware items for this operator.



- In the "Events Window" tab you can choose which columns will be visible in client's events window when logging with this operator.



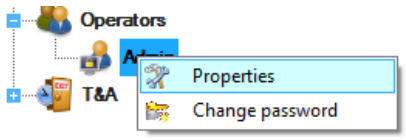
- In the "Hide Maps" tab you can choose which maps will be visible in the client when logging with this operator



- Click on the Add & Exit button

Edit an operator

- Right-click on operator and select Properties menu



- Edit the operator properties in the operator window and click on the Save & Exit button

Delete an operator

- Right-click on the operator and select the Delete menu

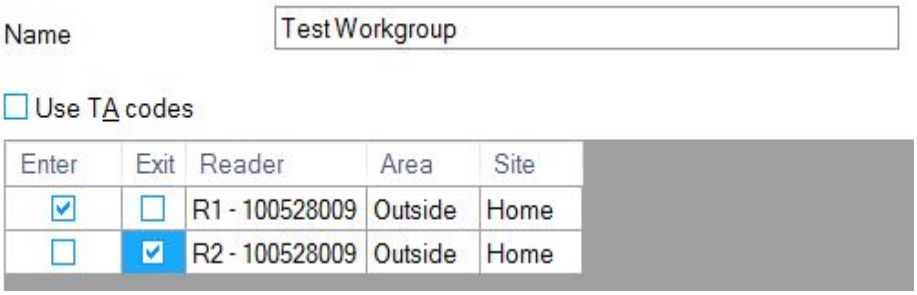
Time and Attendance

Workgroups

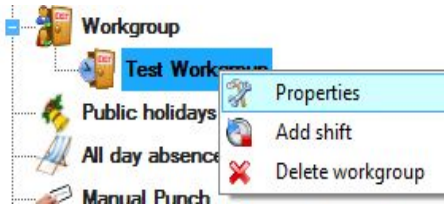
A workgroup is a set of employees that work the same shifts and are registered on the same readers. In any one day, the members of a workgroup do not have to work the same shift, but in any shift defined for the workgroup..

- Right-click on the Workgroup item and select **Add Workgroup**

- Enter the name of the workgroup and select the Entry and Exit readers that this workgroup will use.
    - It is recommended that different readers be used for registration of Entry and Exit.
    - If the same readers are used for registration of Entry and Exit, the readers have to be checked for Enter, and none to be checked for Exit. In this case every following event will be treated as opposite to the previous (if the user has entered, the next registration on the reader will be treated as Exit).

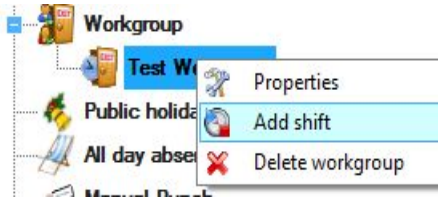


- Click Save & Exit.
- You can edit the workgroup later by right-clicking on the created workgroup and then selecting Properties.

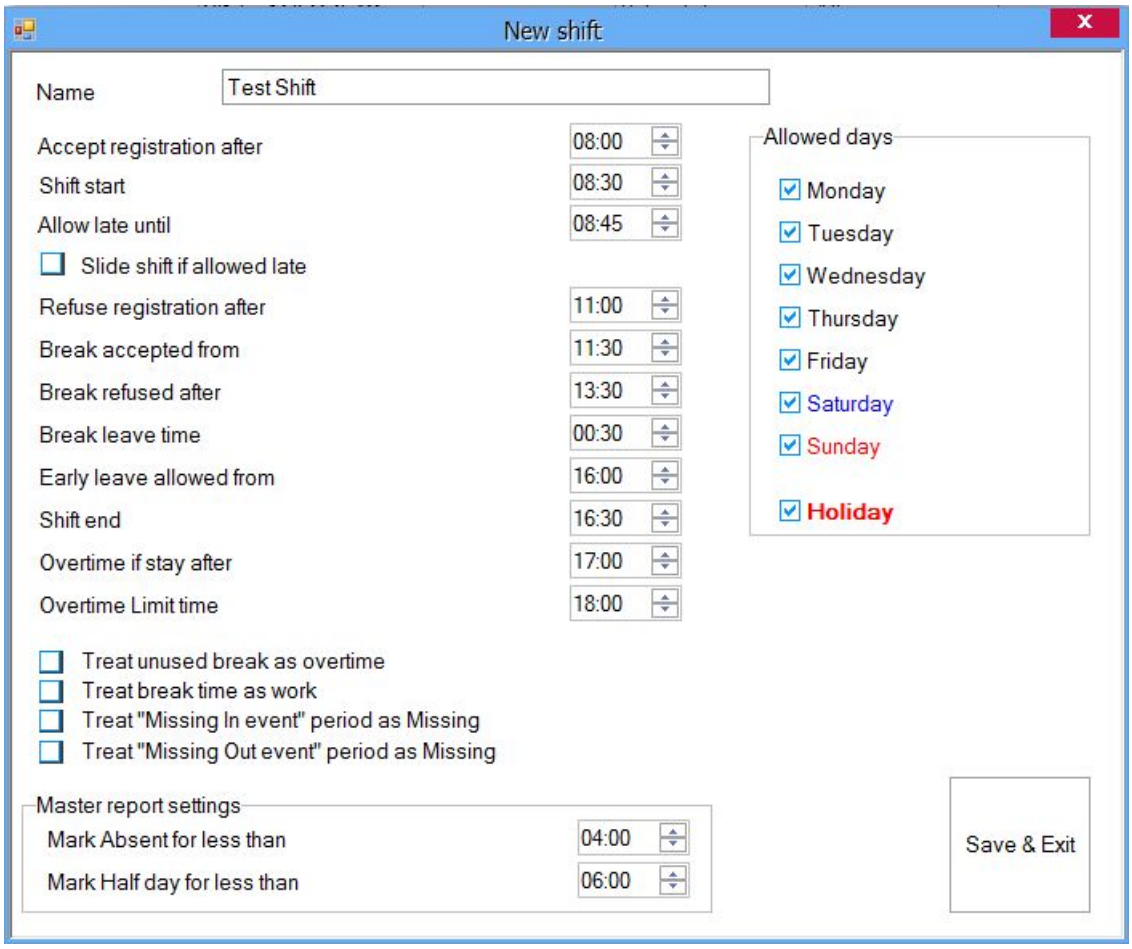


Shifts

- To create a shift for a specific workgroup, right-click on it and select **Add shift**.



- Set the parameters for the shift.

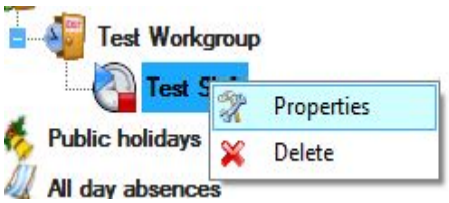


  - Name: Set the name (number) of the shift.
  - Accept registration after: after how long registration of personnel will be treated as the same shift.
  - Shift start: time when the shift starts.
  - Allow late until: permitted delay. A delay within that time limit will not be shown in the reports and working time will be estimated as if the person came on time.
  - Slide shift if allowed late: if the person is no later than the time defined in "Allow late until", the person has to stay after the official end of the shift for the same length of time by which he was late, otherwise the missing period will be treated in the reports as if the person was out.
  - Refuse registration after: registration for the beginning of working hours will not be accepted in this shift. The software will search to see if this registration matches other shifts defined for this workgroup.
  - Break accepted from: at which time the person may take a break.
  - Break refused after: until when the person may report exiting for a break.
  - Break leave time: allowed break time.
  - Early leave allowed from: at which time the person may report end of shift without it being treated as an early leave in the reports.
  - Shift end: end of the shift.
  - Overtime if after: shows the time after which working hours are counted as overtime hours. If the person stays later then this time, the time from the end of the shift to the moment he checks out will be counted as overtime work. If the person leaves before this time the report will show the difference between the end of the shift and his exit as "staying late".
  - Overtime limit time: the person must not stay overtime after this time. If they report the end of shift after this time, the overtime work will be calculated from the end of the shift to the overtime

limit time.
- Treat break time as work: if this option is checked the break time will be added to working hours..
- Treat unused break as overtime:When this option is checked if the person don't leave for break then the break time will be counted as overtime work.
- Treat "Missing In Event" period as Missing: the software calculates periods between two events - Entry and Exit. There are some times when the person may "jump" one event, so there are cases when the person has exited twice without entering. The period between those two events in the reports can be shown as a period when the person was not at work (missing) or as a period for which registration of entry is missing depending on the settings of this option.
- Treat "Missing Out Event" period as Missing: the software calculates periods between two events - Entry and Exit. There are some times when the person may "jump" one event, so there are cases when the person has entered twice without exiting. The period between those two events in the reports can be shown as a period when the person was not at work (missing) or as a period for which registration of entry is missing depending on the settings of this option.
- Master report settings: A user can be marked as being absent or working half day based on the values set in these fields.
- Allowed days: days for which the shift is valid.

- Click Save & Exit

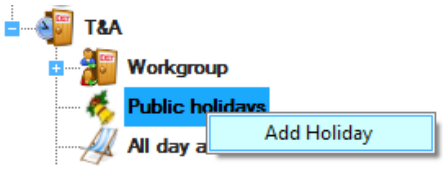
- You can edit the shift later by right-clicking on it and select Properties.



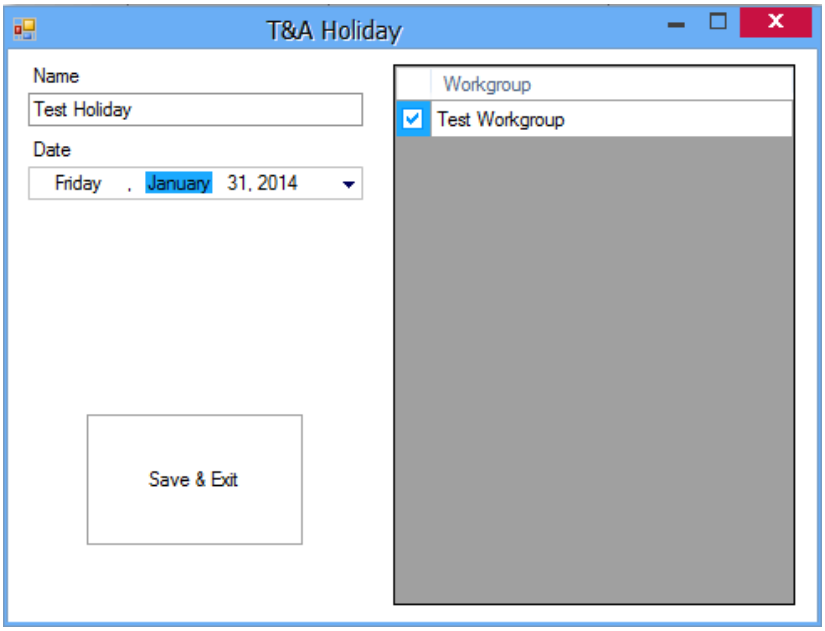
Public holidays

The holiday settings for working hours are separate from the holiday settings for the controllers and they don't influence access control.

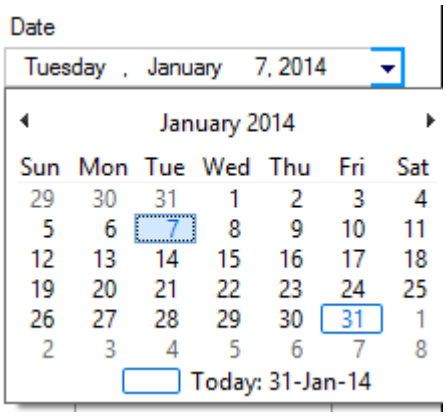
- Right-click on the holiday item and select Add Holiday.



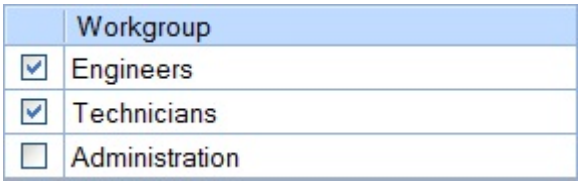
- Set the holiday parameters



- Set the holiday Name
- Set the holiday Date.

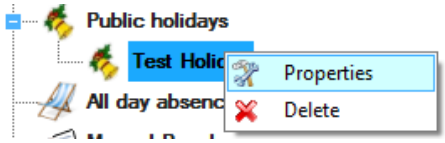


- Check the workgroups for which this holiday is applicable and click on Save & Exit.

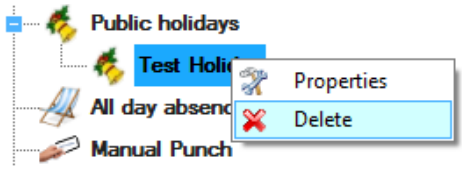


- The holiday will appear under the Public Holidays

- To change holiday properties, right-click on it and select Properties

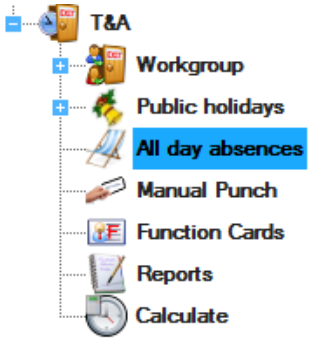


- To delete the holiday, right-click on it and select Delete



All day absences

- Double-click on the **All day absences** item to open the window.

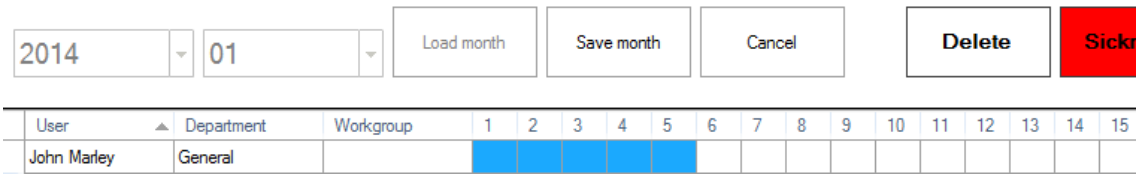


- Select the month you want to see/edit from the list and then click on the Load month button**.**

A list of all users will be shown along with their absences (if they have any).

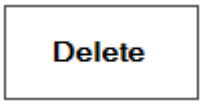
1. Every absence is associated with a specific colour as shown below.

2. To add an absence to a specific user
    - First click on the date you want to mark (if you want to mark more dates, click and drag the mouse over those dates).



- Then click on the colour (absence) you need (for example for Sick - click on the Red coloured box named Sick).

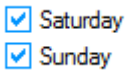
- To delete an absence from a specific user
  - First click on the date you want to mark (if you want to mark more dates, click and drag the mouse over those dates)
  - click on the Delete button.



- To delete ALL absences for all users from the selected month
  - click on the Clear button.

- If you want to save the changes you've made - click on the Save month button otherwise click on Cancel.

- If you want weekend days to be **marked/not marked** when setting absences - **check/uncheck** the boxes respectively, see below.

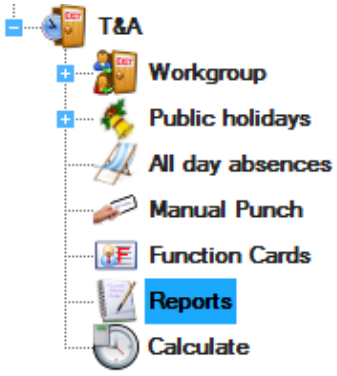


- In order for the absences to appear in the reports, a calculation must be done
  - manual calculation - **Calculate** item from the **T&A** menu
  - Automatic calculation - if set in **Settings > T&A** from the main menu (the calculation will be made within the hour set inAutomatic Calculation).

Reports

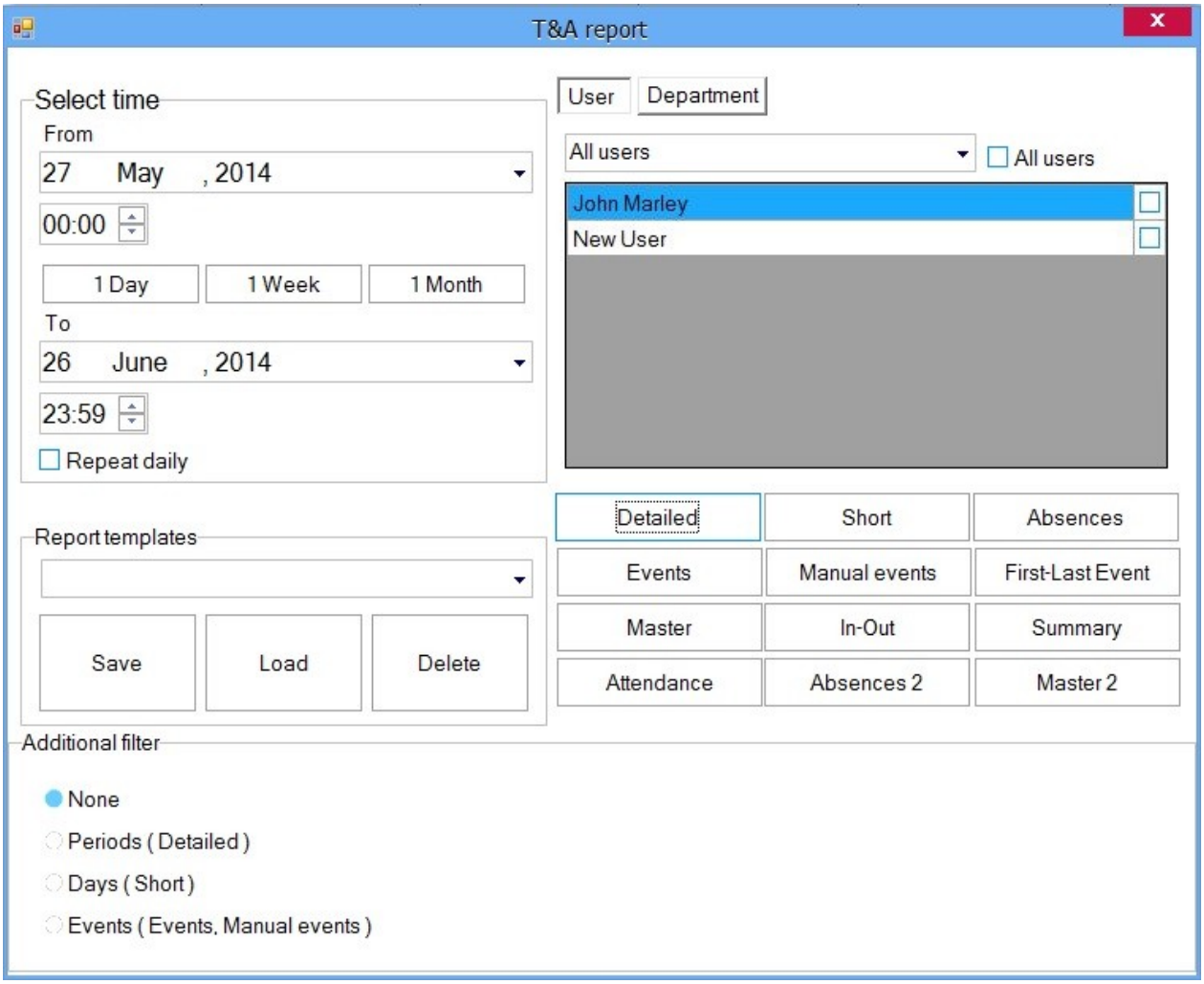
The reports for working hours give estimated cumulative working times for events up until the moment when the last calculation for the working time was made for the corresponding month. In the event that there new events or parameter changes for the working hours (workgroups, shifts, holidays) were made since the last calculation, before generating reports it is necessary to perform a working hour calculation.

- Double-click on the Reports item under T&A to open the T&A reports window.



Edit Reports

- Set the parameters for T&A reports.

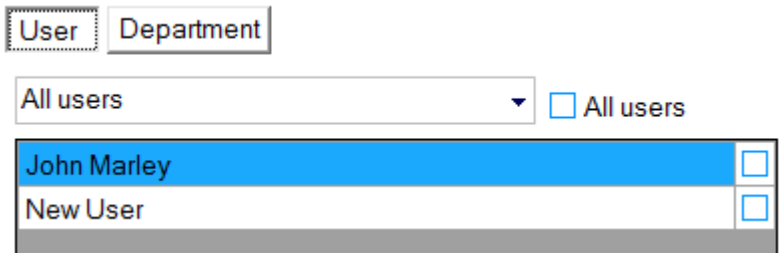


  - Detailed report: this report gives the total number of working hours for one month and for each day separately.
  - Short report: gives the total number of working hours for a whole month.
  - Absences: Gives a list of persons that were absent in selected period.

- Events: Show the events for the selected period
- Manual events: Shows a list of manually added T&A events.
- First/Last Event Report: this report is not included in the calculation of working hours. It gives the first and the last registration of the person on any reader in the system for each day and the time difference between these two events. The report does not calculate the difference if the person works a shift which ends the following day (night shift).
- Master report: Shows a short daily summary report.
- In Out report: Shows informations about start and end of the working day
- Summary report: Shows summary details for a period

User report

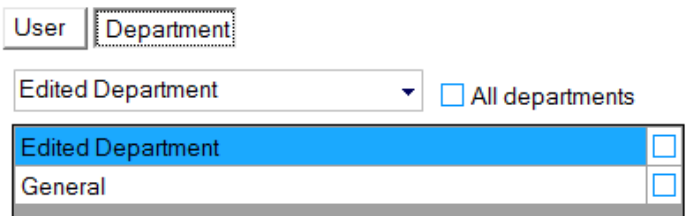
- Select the User tab in the Basic filter panel.



- Select the user from the drop-down list box.
- Check the "All users" item to view a report for all users.
- For more than one user report select users by checking them at check boxes at right side
- Click the Detailed report button to view a detailed list of events for that user.
- Click the Short report button to view a basic list of events for that user.
- Click on Absences button for list of the the persons that were absent on the selected days
- Click on Events button for the event report
- Click First/Last Event Report to view the first and last day event for that user.
- Click Master report button to view the master report for that user.
- Click In-Out report button to view the In-Out report for that user.
- Click Summary report button to view the Summary report for that user.

Department report

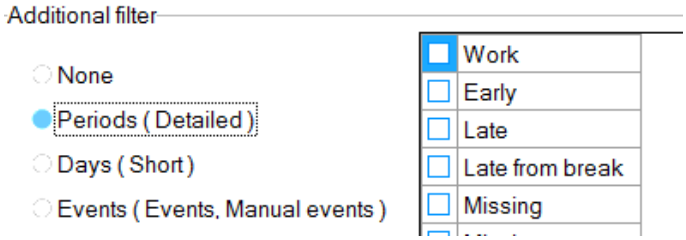
- Select the Department tab in the Basic filter panel.



- Select the department from the drop-down list box.
- Check the "All Departments" item to view a report for all departments.
- For more than one department report select users by checking them at check boxes at right side
- Click the Detailed Report button to view a detailed list of events for that department.
- Click the Short Report button to view a basic list of events for that department.
- Click on Absences button to list the absence by department on the selected days
- Click on Events button for the event report
- Click First/Last Event Report to view the first and last day event for that department.
- Click Master report button to view the master report for that department.
- Click In-Out report button to view the In-Out report for that department.
- Click Summary report button to view the Summary report for that department.

Add a Period filter to reports

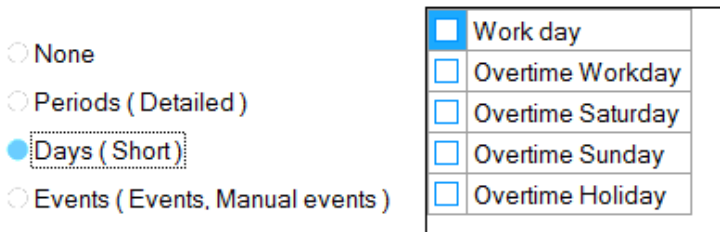
- Select Periods in the Additional filter panel.



- Check the filters in the list that you want to be applied to the report.
- The Periods filter applies only to "Detailed" report

Add a Day filter to reports

- Select Day in the Additional filter panel.



- Check the filters in the list that you want to be applied to the report.
- The Periods filter applies only to "Short" report

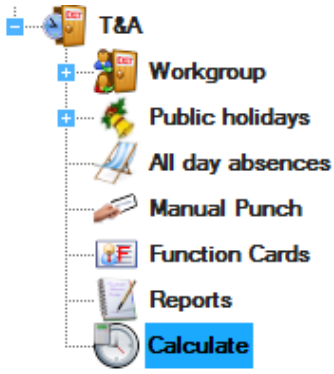
Add a Event filter to report

- Select the Events tab in the Additional filter panel

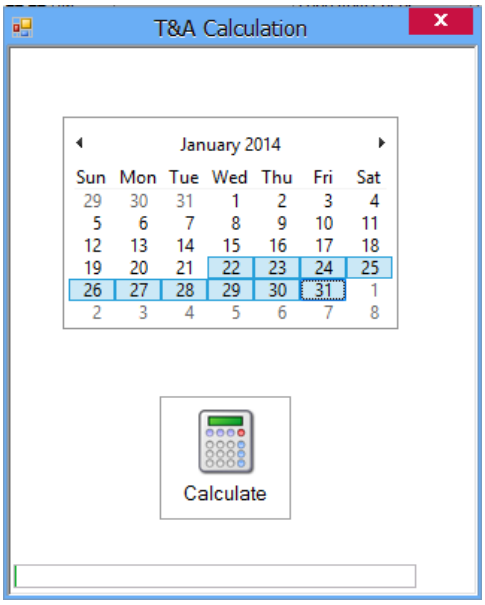
- Check the filters in the list that you want to be applied to the report.
- The Periods filter applies only to "Events" and "Manual Events" reports

Calculation

- Double-click on the Calculate item.



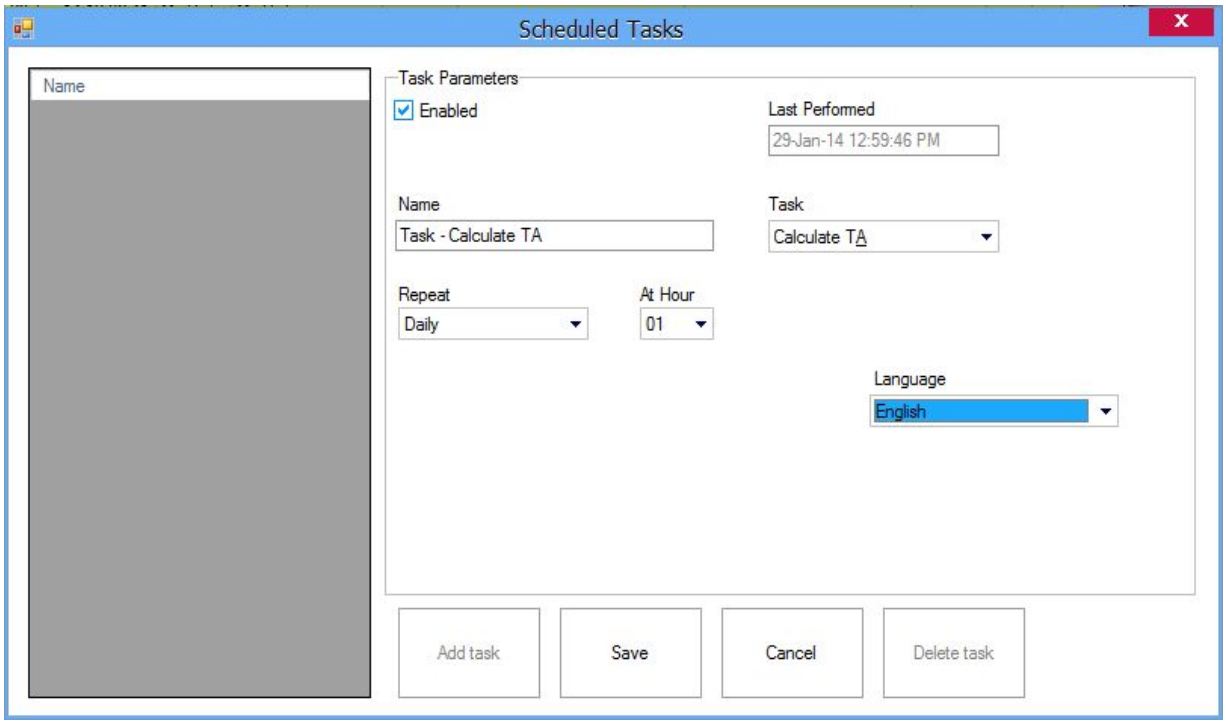
- Select a period and click calculate.
    - This operation calculates working hours based on the registration of a person on the readers.



    - Click and drag over the calendar to select the period for calculation.
    - The calculation can be performed for a period no longer than one month.

Automatic Calculation

- Select **Settings > Scheduled tasks** from the main menu.



- Click on Add task button and fill in the fields the necessary information:
  - Enable field should be checked
  - Enter task Name
  - Set Task to "Calculate T&A"
  - Set Repeat to desired execution period
  - Set the hour during the day for execution.
  - Set Weekday during the week for execution if it is weekly task.
  - Set the day during the month for execution if it is a monthly task.

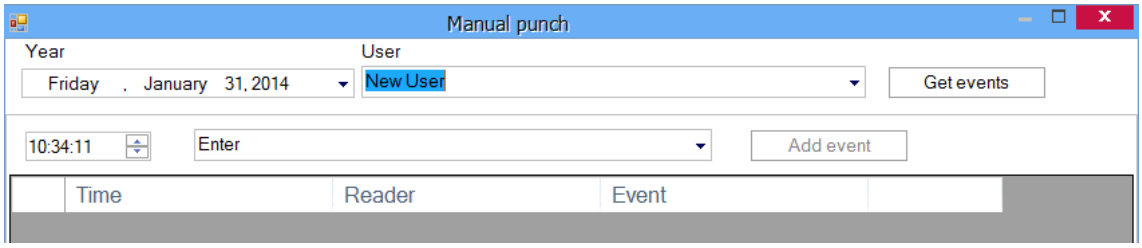
It is possible to create more than one task for T&A calculation based on different periods, like one task as daily and another task as monthly.

NOTE: The Server must be running for automatic calculation to work. For example if the Calculation time is set to 04 hour, the Server must be running from 03:59 to 05:01

Manual Punch

For correction of T&A calculations, manual entry of an access event can be changed using the Manual Punch form.

Double-click on the Manual Punch icon from the T&A list.



1. Select the Date of the event.
2. Select the User for the event.
3. Click on "Get Events". The table will display all the events for this user for the selected date. Rows marked yellow indicate previously added manual events.
4. To add an event, select the time and event type and click on "Add Event". It will be added to the table marked with yellow.

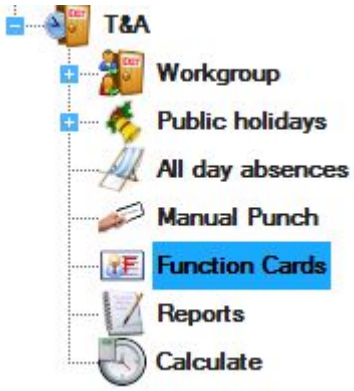
Time	Reader	Event	
11/04/01 11:51:33	BloXrSW	Access granted	
11/04/01 19:25:47	Bio'XrC	Access granted	
11/04/02 08:51:28	BloXrSW	Access granted	
11/04/02 12:12:46	Bio'XrC	Access granted	
11/04/02 17:43:16	Bio'XrC	Access granted	
11/04/03 14:51:57	Enter	Enter	Delete
11/04/05 08:52:23	BloXrSW	Access granted	
11/04/05 10:08:31	Bio'XrC	Access granted	
11/04/05 10:08:58	BloXrSW	Access granted	
11/04/05 10:10:24	Bio'XrC	Access granted	
11/04/05 10:10:54	BloXrSW	Access granted	

5. To delete a manual event, click on the Delete button at the end of the event row. Real events cannot be deleted.

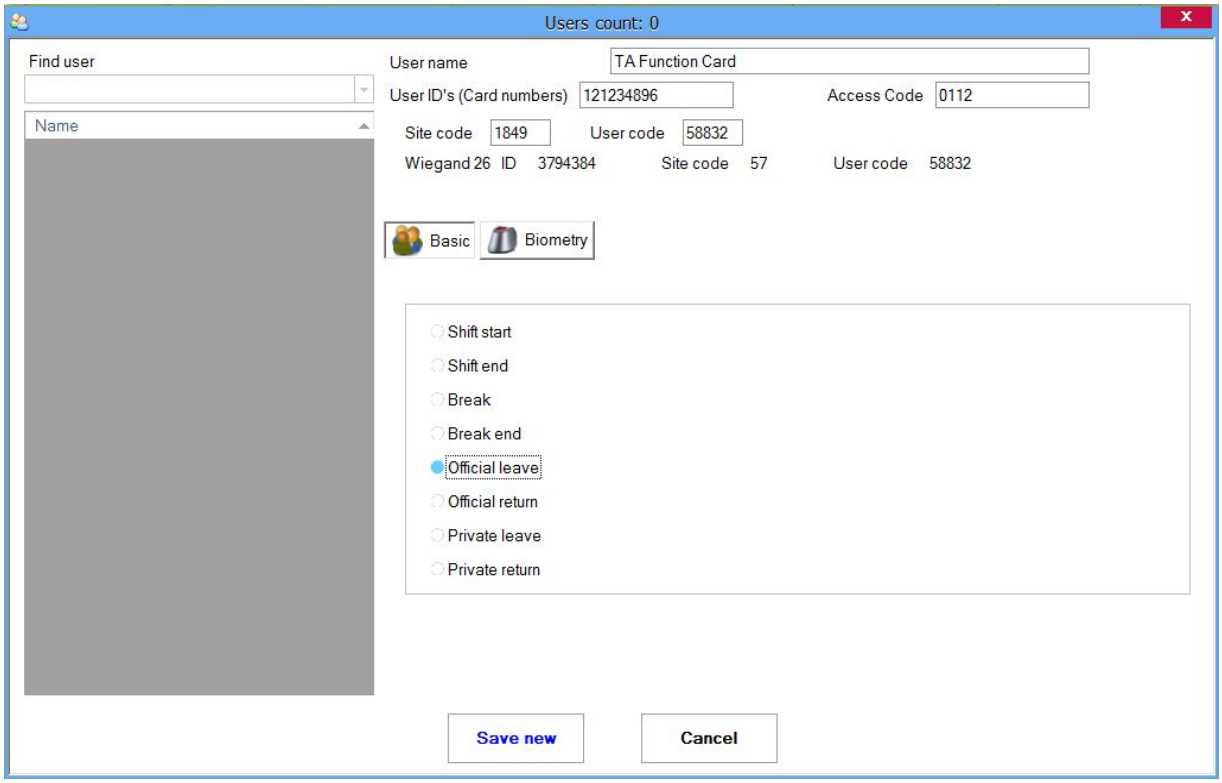
Function cards

Function cards for T&A are used to mark exit as exact T&A event. When checking upon exit for official or private leave the user must first present the Function card then their card to the reader.

Double-click on the Function cards item under the T&A list.



On the Function cards window you can manage cards in the same way as users.



A function card can be used as an access Access Code or Finger print.

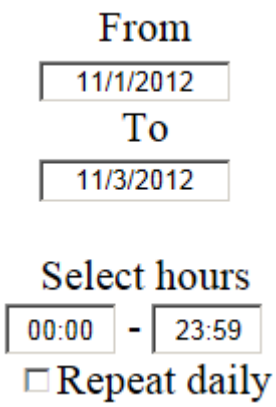
Web report server

Access & Attendance report

Basic filter

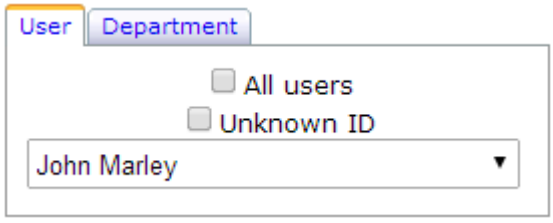
Time filter

- Set the time filter for the report.



- Set the date and the time for the report.
- Repeat daily: If Repeat daily is checked, reports will be generated for the selected time range of the day, every day in the selected days range

User report



- Select the User tab
- Select the user from the drop-down list box.
- For a report of all users check the **All users** box.
- For a report of invalid registration check the **Unknown ID** box.
- Click on Access to generate access report
- Click on some of the reports in the T&A section to generate Time Attendance report

Detailed report: this report gives the total number of working hours for one month and for each day separately.

Short report: gives the total number of working hours for a whole month.

Absences: Gives a list of persons that were absent in selected period.

Events: Show the events for the selected period

Manualevents: Shows a list of manually added T&A events.

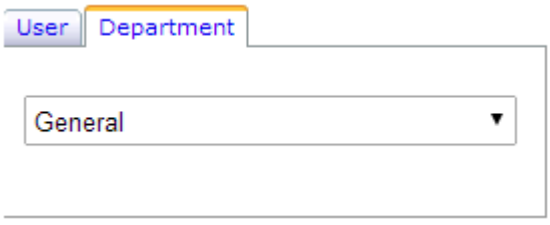
First/Last Event Report: this report is not included in the calculation of working hours. It gives the first and the last registration of the person on any reader in the system for each day and the time difference between these two events. The report does not calculate the difference if the person works a shift which ends the following day (night shift).

Master report: Shows a short daily summary report.

In Out report: Shows informations about start and end of the working day

Summary report: Shows summary details for a period

Department report



- Select the **Department** tab
- Select the department from the drop-down box
- Click on Access to generate access report
- Click on some of the reports in the T&A section to generate Time Attendance report

Detailed report: this report gives the total number of working hours for one month and for each day separately.

Short report: gives the total number of working hours for a whole month.

Absences: Gives a list of persons that were absent in selected period.

Events: Show the events for the selected period

Manual events: Shows a list of manually added T&A events.

First/Last Event Report: this report is not included in the calculation of working hours. It gives the first and the last registration of the person on any reader in the system for each day and the time difference between these two events. The report does not calculate the difference if the person works a shift which ends the following day (night shift).

Master report: Shows a short daily summary report.

In Out report: Shows informations about start and end of the working day

Summary report: Shows summary details for a period

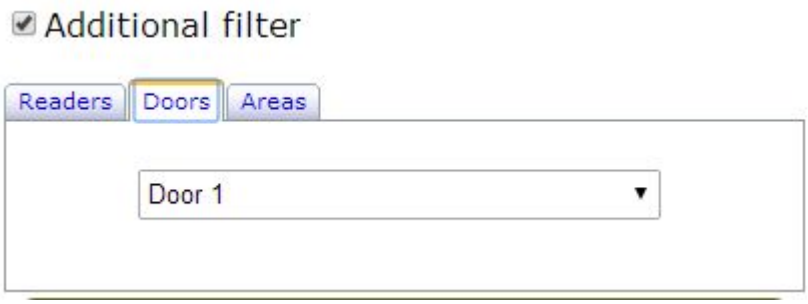
Access additional filter

The additional filter gives an access report for Readers, Doors and Areas. The settings in the Basic filter window are applied for the Additional filter.
Check the Additional filter checkbox to use the additional filter.

- Select the **Readers** tab from the Additional filter window.

- Select the reader from the drop-down box.
- Click **Access** to view the access report for the reader.

- Select the **Doors** tab from the Additional filter window.



- Select the door from the drop-down box.
- Click **Access** to view the access report for the door.

- Select the **Areas** tab from the Additional filter window.

- Select the area from the drop-down box.
- Click **Access** to view the access report for the area.

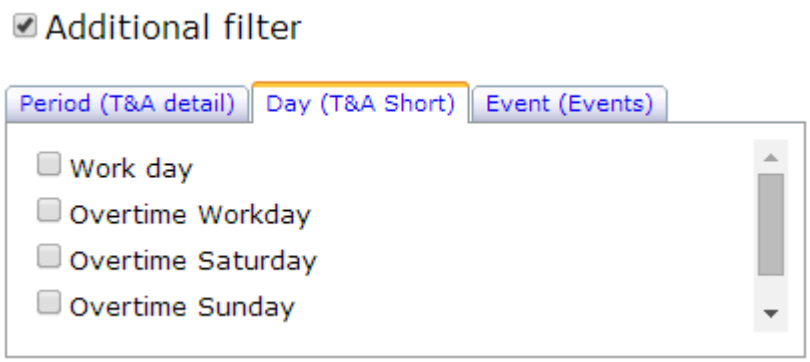
T & A filter

The T&A filter gives a report for the working hours. The settings in the Basic Filter window are applied to this report.
Check the Additional filter checkbox to use the additional filter.

- Select the **Period** tab from the T&A Filter window

- Check the periods for the report
- Click **T&A Detail** to get the report

- Select the **Day** tab from the T&A Filter window



- Check the days for the report
- Click **T&AShort** to get the report

- Select the **Event** tab from the T&A Filter window

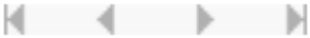
- Check the events for the report
- Click **Events** or **Manual Events** to get the report

Reports options

All reports can be shown on the report form using the following buttons:

- Export - save report to disk or send to email recipient in various file formats (PDF, Excel, Text…). The pop-up blocker on the browser must be disabled!

- Print - print report. The pop-up blocker on the browser must be disabled!

 - Navigation - to view the First page, Previous page, Next page, Last page

- Find - search for specific text in the report.

Troubleshouting

- **EWSi portal (CNV1000) is not found in "Search network portals"**
  1. Check if EWSi is powered
  2. Check if EWSi and the PC are connected to the network
  3. Disable the network firewall
  4. Check the port value in the search window

- **EWSi portal (CNV1000) is found, but can't be configured**
  1. Check if the password in the search window matches the EWSi password. If you forget the password, use the reset button in the EWSi to set the CNV1000 to default values.
  2. Check the port value in the search window
  3. If the PC IP address has a different IP network, set it to the same network, configure the router and restore the PC settings to the previous value.
     - Example:
       - If the PC IP address is 10.10.10.5 and the EWSi IP address is 192.168.1.100, set the PC IP to value 192.168.1.X where X is between 1 and 254, taking care not to set the same address as the EWSi or another existing IP address in the network
       - Configure EWSi
       - Set the PC IP address back to 10.10.10.5

- **EWS does not react on reader reading (Reader's LED stays inactive)**
  1. EWS Wiegand is not set to match the reader
  2. Check the reader power supply
  3. Replace the reader

- **Devices connected to the USB to RS485 converter are offline**
  1. The USB converter is represented as a COM Port on the PC side. If the converter is plugged into another USB port, the COM number will be changed. The solution is to plug the converter into the initial USB port or to change the COM value in the Portal properties.
  2. Check the converter connections

- **Controllers change connection state (controller icon changes background color to red)**
  1. If the controller is using an RS485 connection, check for cable damage, termination load (120 Ohm) and quality of cables
  2. More than 31 units, the controllers and readers are connected to the same RS485 bus

- **Cannot get events report for User**
  1. The user was deleted and entered again with the same name. Once the user is deleted, all events for the user are deleted. Entering a new user with same name will not retrieve the events. The solution is not to delete the user (you can change the access level to "Nowhere" instead) or generate reports for the user and export them to a PDF, Excel or Text file for keeping.

Biometry

- **Reader reading performance is decreased**
  1. Check if the fingerprint reading area is dirty. Do not clean the device with any form of liquid. Use a soft and dry cloth only.
  2. The reading area is damaged. If the damage is minor, try to calibrate the sensor

- **Fingerprint is not recognized normally**
  1. If your finger is wet, retry after drying it.
  2. When your finger is too dry, retry after blowing on your fingertip.

3. If you have a cut on your registered finger, register another fingerprint.

- **Fingerprint is recognized, but EWS reports another ID number**
  1. If the user is not deleted from the reader and the user is enrolled again with a new ID, the reader will recognize the finger with the first ID. To resolve this, delete all users from the reader and re-upload all users to the reader.

Glossary

A

Access Area: A restricted access area controlled by a reader. One area can contain other separate areas, such as one or a group of rooms, parking lot, fenced restricted area...
Access controller: When a credential is presented to a reader, the reader sends the credential's information, usually a number, to a Control panel, a highly reliable processor. The control panel compares the credential's number to an internal access control list, grants or denies the presented request, and sends a transaction log to a database. When access is denied based on the access control list, the door remains locked. If there is a match between the credential and the access control list, the control panel operates a relay that in turn unlocks the door. The control panel also ignores a door open signal to prevent an alarm. Often the reader provides feedback, such as a red LED for access denied and a green LED for access granted. Smart electronics with the ability to remember the User's ID; Time zones; Events; to control Doors; Relays; to receive information about the Door state; Inputs; Readers; to communicate with Access control software and to take action based on events and programmed parameters
Access level: Definition of time zones for each reader. Users can access readers only during the defined time zones in the Access level to which they belong. One user can be assigned to one Access level only. The same time zone can be used in an unlimited number of Access levels.
Anti-passback: Prevention of allowing the user to enter an area more than once with the same ID. It prevents users lending their ID to another person for the purpose of entering the area. This function is useful when a higher level of security is needed, counting the number of persons in areas, time attendance, fire reports, etc. Anti-passback can have more variations. It can be valid for one or more readers, one or more doors, can be reset at a fixed time of the day, can prevent double access within a given period of time. Since the Access controller is enforcing these restrictions, Anti-passback can be enforced only on doors and readers connected to the same controller.

B

Biometry: The way of recognizing specific body parts specific to each person. The most common parts used in security systems are Fingerprint, Face, Eye, Finger vein, Voice and Palm. For higher security, biometry can be mixed and combined with standard access techniques like Fingerprint + Proximity card, Fingerprint + Code.

C

Code: Personal identification presented by typing a sequence of numbers on a keypad. Depending on the keypad model it can be with a fixed or variable length.
COM, COM port: Serial communication interface. Can be an existing PC port or can be an external component. The external component can be a USB device with drivers or a network device using drivers on the PC side to create a virtual COM port.
Control panel: Same as Access controller

D

Department: Grouping the users by internal organization. Used for printing reports with a convenient grouping of users.
Door contact sensor: The sensors are standard magnetic door sensors used in security applications. Either Normally Open or Normally Closed Sensors can be used. Normally Closed sensors (door closed, switch closed) are recommended so that an alarm can be generated if the connection wire breaks.

E

Egress button, Exit switch: Push-button used to open the door from the protected area side. It is connected to the Access controller. Electronic touch sensors can be used with the same function.

Electric strike: An access control device used for doors. It replaces the fixed strike faceplate often used with a latchbar (also known as a *keeper*). Like a fixed strike, it normally presents a ramped surface to the locking

latch allowing the door to close and latch just like a fixed strike would. However, an electric strike's ramped surface can, upon command, pivot out of the way of the latch allowing the door to be pushed open (from the outside) without the latch being retracted (that is, without any operation of the knob) or while exited the knob or lever can be turned to allow egress from the secured area.

Electric strikes generally come in two basic configurations:

- Fail-secure. Also called Fail-locked or non-fail safe. In this configuration, applying electrical current to the strike will cause it to open. In this configuration, the strike would remain locked in the event of a power failure, but typically the knob can still be used to open the door from the inside for egress from the secure side. These units can be powered by AC which will cause the unit to "buzz", or DC power which will offer silent operation, except for a "click" while the unit releases.

- Fail-safe. Also called Fail-open. In this configuration, applying electrical current to the strike will cause it to lock. In this configuration, it operates the same as a magnetic lock would. If there is a power failure, the door would open merely by being pushed/pulled open. Fail safe units are always run using DC power.

F

Fingerprint reader: Reader with the ability to recognize a human finger and send information to the Access controller.
Fire alarm input: Triggering this input will release all doors controlled by the Control panel
Firmware: Programs and data structures that internally control various electronic devices

I

ID: Identification number presented to the Access controller by the Reader. The reader gets information from the media presented (Proximity card, Code, Biometry) and translates it to a number format that the Access controller can recognize.
Input: A hardware gate on the Access controller able to receive information about other equipment. It can be dedicated to a specific task (door monitor, egress button...) or can be programmatically assigned to monitor other devices (Intruder alarm, fire, temperature). The access controller can be programmed to execute specific actions following the change of the inputs state. Inputs can only have two states (OFF/ON). Inputs are also used to pass the information to the Access control software.
IP Address: The **Internet Protocol** (**IP**) **address** is a numerical label that is assigned to devices participating in a computer network that uses the Internet Protocol for communication between its nodes.
IP Port: The port number is a 16-bit unsigned integer, ranging from 0 to 65535. The process associates with a particular port (known as *binding*) to send and receive data, meaning that it will listen for incoming packets whose destination port number and IP destination address match that port, and/or send outgoing packets whose source port number is set to that port.

M

Magnetic lock: A simple locking device that consists of an electromagnet and armature plate. By attaching the electromagnet to the door frame and the armature plate to the door, a current passing through the electromagnet attracts the armature plate holding the door shut.

Mantrap: A group of doors with the logic that only one door can be open at a time. Opening one of the doors leads to the locking of all other doors until the closure of the first one. Using a combination of inputs and outputs, a mantrap can be extended to doors from different Access controllers in the same site.

O

Operator: A person listed in the Access control software with given rights for one or more options.
Output: Additional output available in the Access controller. Not dedicated to primary role of Access control. Can be configured for the execution of some tasks (Timer, Alarm bell, Light control...).

P

Portal: A hardware interface between the Access control software and the devices installed in the system. One portal can connect one or more devices to the software. A portal can exist as a single device or as part of the Access controller.

R

Reader: A device installed near the access barrier (door, gate, turnstile..) to recognize user identification media (card, code, finger..) and to send information to the Access controller.
Relay: An electrical component used as an output by the Access controller. It provides electric isolation between the Access controller and the device that is controlled by the output. The relay has two states: ON and OFF. The output of the relay provides a mechanical switch contact with two outputs - one contact is open when the relay is energized and the other is closed.
.

T

Time zone: The definition of the time period of the day used to later define system behavior by time periods. The time zone also has weekday and holiday definitions as additional filters for system behavior.
Touch sensor: An electronic device that reacts to human touch. Mostly used as an egress button.

W

Wiegand interface: A wiring standard used to connect a card swipe mechanism to the rest of the electronic entry system. A Wiegand-compatible reader is normally connected to a Wiegand-compatible security panel.